Math 40520: Introduction to Number Theory
Lecture Notes

Andrei Jorza

December 2, 2022

Lecture 1
2022-08-24

---

1 Integers in other bases

What does it mean when we say 2022 is written in base 10? We mean that

$$2022 = 2 \cdot 10^3 + 2 \cdot 10 + 2$$
$$2.022 = 2 + 2 \cdot 10^{-2} + 2 \cdot 10^{-3}.$$

More generally, we can write numbers in a base b. If in base 10 the allowed digits are 0,1,...,9, in base b the allowed digits are $0, 1, \ldots, b-1$. To write a number N in base b means to write a sequence of digits $a_d, a_{d-1}, \ldots, a_0 \in \{0, 1, \ldots, b-1\}$

$$\begin{aligned} N &= a_d a_{d-1} \ldots a_1 a_{0(b)} \\ &= a_d b^d + a_{d-1} b^{d-1} + \cdots + a_1 b + a_0. \end{aligned}$$

Here b^d is the largest power of b which is $\leq N$ (keep in mind that the number of digits is $d+1$), and $a_d b^d$ is the largest multiple of this which is $\leq N$, and so on.

For instance, in base 2 the allowed digits are 0 and 1. So $7 = 2^2 + 2 + 1 = 111_{(2)}$ and $9 = 2^3 + 1 = 1001_{(2)}$.

Let's write 2022 in base 2. We seek the largest power of 2 $\leq$ than our number:

$$\begin{aligned} 2022 &= 2^{10} + 998 \\ &= 2^{10} + 2^9 + 586 \\ &\vdots \\ &= 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 2 \\ &= 11111100110_{(2)}. \end{aligned}$$

We can play this game with other bases, let's write 2022 in base 5. The powers of 5 are 1, 5, 125, 625, 3125, so the largest power is $625 = 5^4$. This means 2022 in base 5 will have $4 + 1 = 5$ digits. What is the first digit? The largest multiple of 625 which is ≤ 2022 is $3 \cdot 625$ and we see that

$$\begin{aligned} 2022 &= 3 \cdot 5^4 + 147 \\ &= 3 \cdot 5^4 + 5^3 + 22 \\ &= 3 \cdot 5^4 + 5^3 + 4 \cdot 5 + 2 \\ &= 31042_{(5)}. \end{aligned}$$

Remark 1. If the base is a prime p then we will see later how the digits of N in base p appear in the factorization of $N!$. For instance, $2022 = 31042_{(5)}$ has sum of digits $3+1+0+4+2 = 10$ and when you factor 2022!, the power of 5 that appears is exactly $\dfrac{2022-10}{5-1} = 503$.

A frequently used base is 16, the hexadecimal base. In this case the allowed digits are $0, 1, \ldots, 15$, but since we are used to writing "digits" with a single symbol, it is conventional to write the hexadecimal digits 0, 1, ..., 9, $a = 10$, $b = 11$, $c = 12$, $d = 13$, $e = 14$, $f = 15$. It is convenient to use a computer program to write integers in other bases, and throughout the semester I will use Sage:

```
sage: 2022.str(base=16)
'7e6'
```

Exercise 1. What is the smallest base b in which $one_{(b)}$ makes sense, and what decimal number is it in this base?

Continuing the pattern $a = 10$, $b = 11$, ..., $n = 23$, $o = 24$ we need every digit to be $< b$ so $b \geq 25$. The smallest base is $b = 25$ and the decimal version is

$$one_{(25)} = o \cdot 25^2 + n \cdot 25 + e = 24 \cdot 25^2 + 23 \cdot 25 + 14 = 15589,$$

or using Sage

```
sage: Integer('one', base=25)
15589
```

Lecture 2
2022-08-26

Addition and subtration in base b follows the usual rules of arithmetic. For instance $425_{(7)} + 243_{(7)} = 1001_{(7)}$.

Exercise 2. What is $3^7 - 7$ in base 3? What is $b^7 - 1$ in base b?

Lemma 3. *When adding two numbers in base b, each individual carry is at most 1, and the total number of carries is at most the number of digits of the larger of the two terms being added.*

Proof. Write $m = m_d \ldots m_1 m_{0(b)}$ and $n = n_d \ldots n_1 n_{0(b)}$ (padding with 0-s if n has fewer digits than m). We'll add $m+n$ one digit at a time, showing by induction that the carry can be at most 1. The first addition is $m_0 + n_0$. Since each digit is $\leq b-1$, the sum is $\leq 2b-2 = b+(b-2)$ so at most 1 gets carried. Suppose we showed the carry is at most 1 for the first $k-1$ digits and we are now adding the k-th digits. By the inductive hypothesis, the carry from $k-1$ is at most 1, so we are adding $m_k + n_k + \text{carry} \leq b-1+b-1+1 \leq b+(b-1)$ so the k-th carry is at most 1 again. □

Exercise 4. We saw that adding $425_{(7)} + 243_{(7)} = 1001_{(7)}$ has 3 carries. The two numbers are 215 and 129 in base 10, adding to 344 in base 10. We'll see later that the number of carries shows up in the factorization of $\binom{344}{215} = \binom{344}{129}$:

```
sage: binomial(344,129)
3041545100359741635104710429624019512720181047086467407078618406367982852412006766115621002860971 2
sage: binomial(344,129).factor()
2^4 * 3^4 * 7^3 * 11 * 13^2 * 17^2 * 19 * 31 * 37 * 47 * 67 * 73 * 79 * 83 * 109 * 113 * 131 * 137
    * 139 * 149 * 151 * 157 * 163 * 167 * 223 * 227 * 229 * 233 * 239 * 241 * 251 * 257 * 263 * 269
     * 271 * 277 * 281 * 283 * 293 * 307 * 311 * 313 * 317 * 331 * 337
```

So what about the number of digits of N? We know that if b^d is the largest exponent of the base $\leq N$ then N has $d+1$ digits.

Exercise 5. How many digits does 2^{1000} have in base 10?

Proof. We see $10^d \leq 2^{1000}$ so $d \leq 1000 \log_{10}(2) = 301.0290\ldots$ so it has 302 digits. □

Exercise 6. How many digits does the one millionth Fibonacci number have?

Proof. The Fibonacci numbers are $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. The sequence is $0, 1, 1, 2, 3, 5, 8, 13, \ldots$. We'll derive a formula for F_n, that will give us the number of digits, using matrices in a way that will be useful for gcd-s as well.

Let's look at two consecutive Fibonacci numbers $v_n = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$. Then

$$v_{n+1} = \begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n+1} + F_n \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = Av_n$$

where $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Doing this many times we see that

$$v_n = A^n v_0 = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

so finding the Fibonacci numbers comes down to computing the exponents A^n of the matrix A.

In linear algebra we learn that matrices can always be upper-triangularized, and sometimes diagonalized. (Jordan form. Distinct eigenvalues.) The characteristic polynomial of A is $\det(X \cdot I_2 - A) = \det \begin{pmatrix} X-1 & -1 \\ -1 & X \end{pmatrix} = X^2 - X - 1$, whose roots are $\rho = \frac{1+\sqrt{5}}{2}$ (the golden ratio) and $\overline{\rho} = \frac{1-\sqrt{5}}{2} = 1 - \rho$. These two eigenvalues are distinct, so A can be diagonalized. We'll use Sage:

```
sage: K = NumberField(x^2-x-1,'r')
sage: r = K.gen()
sage: A = matrix(K, [[1,1],[1,0]])
sage: A.diagonalization()
(
[    r     0]  [    1     1]
[    0 -r + 1], [r - 1  -r]
)
```

Which means that

$$A = S \begin{pmatrix} \rho & \\ & \overline{\rho} \end{pmatrix} S^{-1} \qquad\qquad S = \begin{pmatrix} 1 & 1 \\ -\overline{\rho} & -\rho \end{pmatrix}.$$

Exponentiating we get

$$A^n = S \begin{pmatrix} \rho^n & \\ & \overline{\rho}^n \end{pmatrix} S^{-1}$$

and so

$$F_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \end{pmatrix} S}_{\begin{pmatrix} -\overline{\rho} & -\rho \end{pmatrix}} \begin{pmatrix} \rho^n & \\ & \overline{\rho}^n \end{pmatrix} \underbrace{S^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\frac{1}{\rho - \overline{\rho}} \begin{pmatrix} \rho \\ -\overline{\rho} \end{pmatrix}} = \frac{\rho^n - \overline{\rho}^n}{\rho - \overline{\rho}}.$$

Since $\overline{\rho} \approx -0.618$ it follows that $\overline{\rho}^{10^6} \approx 0$ so

$$F_{10^6} \approx \frac{\rho^{10^6}}{\sqrt{5}} \qquad \log_{10}(F_{10^6}) = 10^6 \log_{10}(\rho) - \log_{10}(\sqrt{5}) \approx 208987.29$$

so F_{10^6} has 208988 digits. □

Lecture 3
2022-08-29

---

2 Primes and Divisibility

This corresponds to chapter 1 in the textbook.

We are all familiar with the notion of divisibility:

Definition 7. We say that $a \mid b$ if $ac = b$ for some c. Here a, b, c are integers, but this notion makes sense in abstract algebra when using "rings".

Example 8. Let's show that $2^n - 1 \mid 2^m - 1$ whenever $n \mid m$. (In fact this is an if and only if, as we'll see later.)

Indeed, if $n \mid m$ then $nd = m$ for some integer d and we see that

$$2^m - 1 = (2^n)^d - 1 = (2^n - 1)(2^{n(d-1)} + \cdots + 2^{2n} + 2^n + 1)$$

from the usual geometric series formula $x^d - 1 = (x-1)(x^{d-1} + \cdots + x^2 + x + 1)$.

Problem 9 (Challenge question)**.** Suppose you have two integers a, b with the property that $a^n - 1 \mid b^n - 1$. The previous example shows that this is always the case when $b = a^k$ for some $k \geq 0$. It is knows that if the property is satisfied for all exponents $n \geq 1$ then b must be a power of a. This has an elementary argument, which I don't know.

The main theorem about divisibility is

Theorem 10 (Unique factorization)**.** *Every positive integer n can be factored uniquely into primes*

$$n = p_1^{k_1} \cdots p_r^{k_r}.$$

Let's try to probe our intuition in such a way that we'll be able to understand this theorem in its proper context. (In particular, we might get to show a similar theorem when we consider not only integers, but also the complex number i.)

2.1 What is a prime?

What is a prime number? **Answer 1:** A prime number is a positive number $p > 1$ whose only divisors are 1 and p. A different way to say this is that the equation $p = xy$ with $x, y \in \mathbb{Z}$ has as positive solutions only $(1, p)$ and $(p, 1)$.

A few big questions about primes that we'll explore this semester:

1. How many primes are there $\leq X$? We denote $\pi(x)$ the number of primes $p \leq X$. For instance, $\pi(10) = 4$, etc.

   It turns out that $\pi(x) \sim \dfrac{x}{\log x}$ (in this class log = ln). This is an ok approximation, and we'll show something close to it in this course. A much better approximation is $\pi(x) \sim \displaystyle\int_2^x \frac{dy}{\log(y)}$. It is a useful exercise in integration by parts to show that the latter formula approximates the former.

2. Since $\pi(x)$ counts the number of primes among the first x positive numbers, a different way of stating the above approximation is that

   $$\Pr(p \leq x \mid p \text{ is prime}) = \frac{\pi(x)}{x} \approx \frac{1}{\log(x)}.$$

3. How randomly are primes distributed? Are there special types of primes? In the introductory overview we saw in Ulam's spiral the existence of many primes of the form $4n^2 - 2n + 41$. Can we make sense of this?

2.2 Factoring into primes

The first part of Theorem 10 is that every positive integer can be factored into primes. Why is this the case?

For instance, if we start with 12, we see that it's not a prime. In fact 2 and 3 are divisors so we can write $12 = 2 \cdot 6$ or $3 \cdot 4$. The second factor in each case is not a prime, 2 being a divisor, so we can continue the factoring to get $12 = 2 \cdot 2 \cdot 3$ and $12 = 3 \cdot 2 \cdot 2$.

This algorithmic construction of the factorization works in general. (I didn't write this formally during lecture.)

Algorithm for factorization:

1. Start with $n = n$.
2. At step k, we start with a formula $n = x_1 x_2 \dots x_k$, a product with k factors > 1. If all the factors x_i are prime, then we stop. Otherwise, say x_k, is not a prime, so it has a proper divisor x'_k and we write $x_k = x'_k x_{k+1}$ where $x'_k, x_{k+1} > 1$.
3. Since in each step k, $x'_k, x_{k+1} < x_k$ it follows that the non-prime factors in $n = \prod x_j$ decrease. Since positive integers can't decrease indefinitely, the process must stop and $n = \prod x_j$ in the last step must be a prime factorization.

2.3 Uniqueness of factorization

We arrive at the last unexamined aspect of Theorem 10, namely why prime factorizations are unique. For instance, suppose $pq = rs$ are products of primes. Why does this mean that $\{p, q\} = \{r, s\}$?

Answer from class: Divide both sides by r.

This is great intuition but it relies on the following result:

Lemma 11. *Suppose r is a prime. If $r \mid ab$ then $r \mid a$ or $r \mid b$.*

Suppose we know this lemma. Then we can start with $pq = rs$, $r \mid pq$ so by Lemma 11 it must be that $r \mid p$ or $r \mid q$. Say $r \mid p$. Since p is a prime, its only divisors are 1 and p, but $r > 1$ so $r = p$.

Argument for uniqueness of factorization: (I didn't write this formally during lecture.)

1. Suppose $p_1 \cdots p_r = q_1 \cdots q_t$ are two prime factorizations. Then $q_1 \mid p_1 \cdots p_r$ so Lemma 11, just like in the example above, implies that q_1 must be one of the primes p_i.
2. Cancel the same prime from both sides, and repeat.
3. The total number of primes keeps decreasing, so after finitely many steps we finish checking that the two sides are equal.

Remark 2. In fact, in general Lemma 11 is used as a definition of "prime", and the definition with divisors is referred to as "irreducible". The two notions don't coincide in general, but in any setting where they do, one can show unique factorization.

2.4 Gcd and the Euclidean algorithm

Lemma 11 is the principal tool for showing uniqueness of factorization, but it is subtle because it related a question about divisors (primality) to a question about multiples. How does one turn a random number a into a divisor of a number r? The answer comes from computing greatest common divisors.

We denote (a, b) the gcd of a and b. Eg, $(9, 6) = 3$, etc. Computing gcd in practice is very fast and easy, using division with remainder and the Euclidean algorithm. What is division with remainder? For any integers a, b with $b > 0$ we can find a quotient q and a remainder r such that

$$a = bq + r \qquad\qquad 0 \leq r < b.$$

There is nothing mysterious about this. Dividing by b this is the same as

$$\frac{a}{b} = q + \frac{r}{b} \qquad\qquad 0 \leq \frac{r}{b} < 1.$$

So $q = \lfloor \frac{a}{b} \rfloor$ is the integer part and $\frac{r}{b} = \{\frac{a}{b}\}$ is the fractional part.

Lemma 12. *Suppose $a = bq + r$ is division with remainder. Then $(a, b) = (b, r)$.*

Proof. Forget about greatest common divisors, we'll show that the pairs (a, b) and (b, r) have exactly the same divisors, and therefore the same gcds.

Suppose $d \mid a, b$. Then d must also divide $a - bq = r$. Similarly, if $d \mid b, r$ then d must also divide $a = bq + r$. □

Example 13. We can use the Euclidean algorithm over and over to compute gcds. For instance,

$$\begin{aligned} 96 &= 11 \cdot 8 + 8 & (96, 11) &= (11, 8) \\ 11 &= 8 \cdot 1 + 3 & (11, 8) &= (8, 3) \\ 8 &= 3 \cdot 2 + 2 & (8, 3) &= (3, 2) \\ 3 &= 2 \cdot 1 + 1 & (3, 2) &= (2, 1) \\ 2 &= 2 \cdot 1 + 0 & (2, 1) &= (1, 0) = 1. \end{aligned}$$

The Euclidean algorithm can actually give a lot more information, which will be crucial is all kinds of settings.

Theorem 14 (Bézout's formula/Extended Euclidean Algorithm)**.** *Suppose a, b are two integers. Then $(a, b) \mid ax + by$ for all $x, y \in \mathbb{Z}$. Moreover, there exist $x, y \in \mathbb{Z}$ such that*

$$(a, b) = ax + by.$$

How would this work in practice? We could try to look at the divisions from the previous example, and work backwards:

$$\begin{aligned} 1 &= 1 & 1 &= 3 - 2 \cdot 1 \\ &= 3 - 2 \cdot 1 & 2 &= 8 - 3 \cdot 2 \\ &= 3 - (8 - 3 \cdot 2) \cdot 1 = 8 \cdot (-1) + 3 \cdot 3 & 3 &= 11 - 8 \cdot 1 \\ &= 8 \cdot (-1) + (11 - 8 \cdot 1) \cdot 3 = 11 \cdot 3 + 8 \cdot (-4) & 8 &= 96 - 11 \cdot 8 \\ &= 11 \cdot 3 + (96 - 11 \cdot 8) \cdot (-4) = 96 \cdot (-4) + 11 \cdot 35. \end{aligned}$$

Remark 3. This is nightmarish, though straighforward. As it often is the case, the secret to carrying horrible computations successfully to the end depends on the choice of data structure to store your intermediary computations. We'll see next time how to use linear algebra, as we saw in the case of the Fibonacci sequence, to execute these computations in general.

We are now in the position to prove Lemma 11.

Proof of Lemma 11. The direction $r \mid a$ or $r \mid b$ implies $r \mid ab$ is clear from the definition. Suppose now that $r \mid ab$, but $r \nmid a$. We'd like to show that $r \mid b$.

What is (r, a)? On the one hand, $(r, a) \mid r$ so it must be 1 or r. On the other hand, $r \nmid a$, so $(r, a) \neq r$ as $(r, a) \mid a$ by definition. This means $(r, a) = 1$. We now use Bézout's formula to concoct two integers x, y such that $1 = (r, a) = rx + ay$.

Let's look back at what we are given and asked. We are given $r \mid ab$ and asked to show $r \mid b$. But at this moment we only have $rx + ay = 1$. There's a convenient way to put both b and ab into this formula, by multiplying with b:

$$rxb + aby = b.$$

But $r \mid r$ and $r \mid ab$ so r divides the LHS, so it must divide the RHS as well: $r \mid b$. □

Lecture 4
2022-08-31

2.5 Proof of Bézout's formula

Last time we saw how to use the Euclidean algorithm to compute gcds recursively.

1. Start with a, b and write $a = bq_1 + r_1$ division with remainder, giving $(a, b) = (b, r_1)$.
2. Write $b = r_1q_2 + r_2$ giving $(b, r_1) = (r_1, r_2)$.
3. Given r_{k-1} and r_k, divide with remainder to get $r_{k-1} = r_kq_{k+1} + r_{k+1}$ with $(r_{k-1}, r_k) = (r_k, r_{k+1})$.
4. The numbers keep getting smaller until $r_{k+1} = 0$ for some index k, in which case

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_k, 0) = r_k.$$

In summary, we have a sequence (r_n) given by the recursion $r_{n+1} = r_{n-1} - r_nq_{n+1}$, and we need to compute its last nonzero term. How did we deal with linear recursions in the context of the Fibonacci sequence? By putting consecutive terms into a column matrix.

How do we rewrite $r_{n+1} = r_{n-1} - r_nq_{n+1}$ using column matrices?

$$\begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = \begin{pmatrix} -q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ r_{n-1} \end{pmatrix}.$$

Rewriting all the divisions with remainder we get

$$\begin{aligned}
a &= bq_1 + r_1 & \begin{pmatrix} r_1 \\ b \end{pmatrix} &= \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} \\
b &= r_1q_2 + r_2 & \begin{pmatrix} r_2 \\ r_1 \end{pmatrix} &= \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ b \end{pmatrix} = \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} \\
&\vdots \\
r_{n-1} &= r_nq_{n+1} + 0 & \begin{pmatrix} 0 \\ r_n \end{pmatrix} &= \begin{pmatrix} -q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix}
\end{aligned}$$

Multiplying the matrices we get

$$\begin{pmatrix} 0 \\ r_n \end{pmatrix} = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix}$$

from which we see that

$$(a, b) = r_n = zb + ta.$$

This is Bézout's formula.

Example 15. We've already seen how to compute $(96, 11)$, with quotients $8, 1, 2, 1, 1$ so

$$\begin{aligned}
\begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -8 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 11 \\ 96 \end{pmatrix} \\
&= \begin{pmatrix} -61 & 7 \\ 35 & -4 \end{pmatrix} \begin{pmatrix} 11 \\ 96 \end{pmatrix}.
\end{aligned}$$

Alternatively:

```
sage: xgcd(96,11)
(1, -4, 35)
```

This algorithm for explicit Bézout relies only on division with remainder, and therefore works in any context in which one has access to division with remainder.

Example 16. Consider $P(X) = X(X+1)(X-2) = X^3 - X^2 - 2X$ and $Q(X) = (X+1)^2 = X^2 + 2X + 1$. Visibly $(P(X), Q(X)) = X + 1$ and Bézout suggests that we should be able to find two polynomials $A(X)$ and $B(X)$ such that $P(X)A(X) + Q(X)B(X) = (P(X), Q(X)) = X + 1$.

Let's work out the Euclidean algorithm:

$$P(X) = Q(X)(X-3) + 3X + 3$$
$$Q(X) = (3X+3)(\frac{1}{3}X + \frac{1}{3}) + 0.$$

This gives

$$\begin{pmatrix} 0 \\ 3(X+1) \end{pmatrix} = \begin{pmatrix} -\frac{1}{3}(X+1) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -X+3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Q(X) \\ P(X) \end{pmatrix} = \begin{pmatrix} \frac{1}{3}(X^2 - 2X) & -\frac{1}{3}(X+1) \\ -X+3 & 1 \end{pmatrix} \begin{pmatrix} Q(X) \\ P(X) \end{pmatrix}$$

and, equating the two matrices and dividing by 3, we get

$$P(X) \cdot \frac{1}{3} + Q(X) \cdot \frac{1}{3}(-X+3) = X + 1.$$

And now an example where we can apply the Euclidean algorithm in a general situation where we do not have explicit computations.

Example 17. Let's show that $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$ using the Euclidean algorithm.

We won't be able to do actual computations, but we will be able to run the two gcd computations in parallel.

Let $m = nq + r$ with $0 \leq r < n$, for which we know that $(m, n) = (n, r)$. Could we possibly execute division with remainder for $2^m - 1$ divided by $2^n - 1$? We can:

$$\begin{aligned} 2^m - 1 &= 2^{nq+r} - 1 \\ &= 2^{nq+r} - 2^r + 2^r - 1 \\ &= (2^{nq} - 1) \cdot 2^r + 2^r - 1 \\ &= (2^n - 1) \underbrace{(2^{n(q-1)} + \cdots + 2^n + 1) \cdot 2^r}_{Q} + \underbrace{2^r - 1}_{R}. \end{aligned}$$

This is division with remainder because $R = 2^r - 1 < 2^n - 1$ as $r < n$ to begin with. The Euclidean algorithm then gives

$$(2^m - 1, 2^n - 1) = (2^n - 1, 2^r - 1).$$

There's now two ways to finish off.

1. We can run completely the Euclidean algorithm for $(m, n) = (n, r_1) = \ldots = (r_k, 0)$ and then get $(2^m - 1, 2^n - 1) = (2^n - 1, 2^{r_1} - 1) = \ldots = (2^{r_k} - 1, 2^0 - 1) = (2^{r_k} - 1, 0)$ to show that

$$(2^m - 1, 2^n - 1) = 2^{r_k} - 1 = 2^{(m,n)} - 1.$$

2. Alternatively, we can argue by induction on $m + n$. Suppose we know that $(2^u - 1, 2^v - 1) = 2^{(u,v)} - 1$ whenever $u + v < m + n$. Then, because $m + n > n + r$ we have

$$(2^m - 1, 2^n - 1) = (2^n - 1, 2^r - 1) = 2^{(n,r)} - 1 = 2^{(m,n)} - 1.$$

We just need to check the base case, which can be taken to be $m + n = 2$ so $m = n = 1$.

Lecture 5
2022-09-02

2.6 Solving linear equations

Bézout's theorem guarantees the existence of integers x and y such that $ax + by = (a, b)$. Can we solve completely such linear solutions?

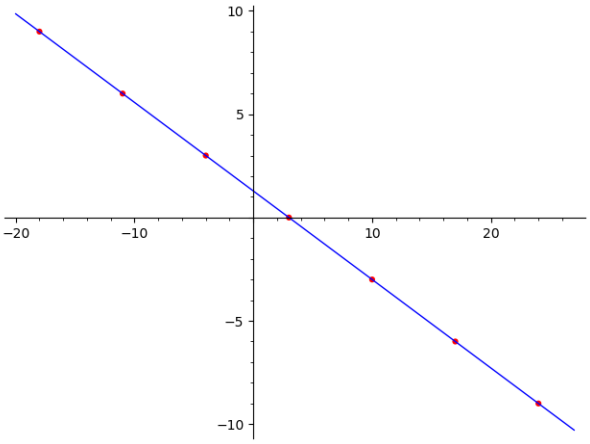
Proposition 18. *Let $a, b, c \in \mathbb{Z}$.*

1. *The equation $ax + by = c$ has a solution with $x, y \in \mathbb{Z}$ if and only if $(a, b) \mid c$.*
2. *If $(a, b) = 1$ and $ax_0 + by_0 = c$ is a solution from the previous part, show that every solution to $ax + by = c$ is of the form $(x_0, y_0) + n(b, -a)$ where $n \in \mathbb{Z}$.*
3. *If $(a, b) \neq 1$, divide by (a, b) and get the equivalent equation $\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = \frac{c}{(a,b)}$, with the two coefficient coprime.*

Example 19. Let's solve the following equations:

$$6x + 9y = 7 \qquad 3x + 7y = 9 \qquad 6x + 9y = 15.$$

Certainly the first equation has no integral solutions as $(6, 9) \nmid 7$. What about the second equation? Bézout gives $3 \cdot (-2) + 7 \cdot 1 = 1$ so we can rescale to get $3 \cdot (-18) + 7 \cdot 9 = 9$. Then every other solution is of the form $(-18 + 7n, 9 - 3n)$ for integers n. It's worth plotting these solutions on the (real) line $3x + 7y = 9$ (what does this line look like?).



Finally, what about the last equation $6x + 9y = 15$? We simply divide by 3 and get to the equation $2x + 3y = 5$. Try it out!

Proof of Proposition. (1): Since $(a, b) \mid a, b$ it follows that $(a, b) \mid ax + by$ for all $x, y \in \mathbb{Z}$. This means that if $ax + by = c$ has a solution, it must be that $(a, b) \mid c$. Suppose now that $(a, b) \mid c$. By Bézout, we can always find integers u and v such that $au + bv = 1$. Multiply by c to get $a(cu) + b(cv) = c$ to get the solution $x_0 = cu$ and $y_0 = cv$.

(2): We start with $ax_0 + by_0 = c$ and try to solve $ax + by = c = ax_0 + by_0$. We get $a(x - x_0) = -b(y - y_0)$. Since $(a, b) = 1$ and $b \mid a(x - x_0)$ it must be that $b \mid x - x_0$. So we can find an integer n such that $x - x_0 = bn$. Pluggin in, we get $a(x - x_0) = abn = -b(y - y_0)$ so $y - y_0 = -bn$. □

Lecture 6
2022-09-05

2.7 Gcd and lcm via prime factorizations

Now that we know that unique factorization into primes works, we can ask whether gcd and lcm are conveniently expressed in terms of the prime factors directly.

Lemma 20. *Suppose a and b are two positive integers. We'll denote by $p_1, \ldots, p_n$ the prime factors of a and b taken together, in which case we can factor $a = p_1^{r_1} \cdots p_n^{r_n}$ and $b = p_1^{s_1} \cdots p_n^{s_n}$. Here the exponents are $r_j, s_j \geq 0$. Then $a \mid b$ if and only if $r_1 \leq s_1, \ldots, r_n \leq s_n$ and therefore*

$$(a, b) = p_1^{\min(r_1, s_1)} \cdots p_n^{\min(r_n, s_n)}$$
$$[a, b] = p_1^{\max(r_1, s_1)} \cdots p_n^{\max(r_n, s_n)}.$$

Problem 21. Is there a quick way to compute lcm the way we computed gcd? Indeed, there is, $(a, b)[a, b] = ab$, which follows from Lemma 20.

Corollary 22. *How many divisors does $a = \prod p_j^{r_j}$ have? Any divisor has to be of the form $\prod p_j^{k_j}$ with $0 \leq k_j \leq r_j$, and each choice of exponent is independent of the others. Therefore we multiply the $r_1 + 1$ choices for the first exponent with the $r_2 + 1$ choices for the second exponent etc. The number of (positive) divisors of a is then*

$$\tau(a) = (r_1 + 1)(r_2 + 1) \cdots (r_n + 1).$$

We are now in the position to answer the math problem I stated on the first day of class:

Problem 23. Suppose you have 2022 light switches in a room, labeled 1, 2,..., 2022, all in the off position. For each d from 1 to 2022, you flip every light switch whose label is a multiple of d. How many light switches are on at the end?

Proof. Let's look at light switches at the very end. How many times was a switch labeled n flipped? It gets flipped every time n is a multiple of the d in step d. This means that each switch n is flipped exactly $\tau(n)$ times. Since each switch starts in the off position, switch n is "on" at the end precisely when it was flipped an odd number of times. In other words, if $\tau(n)$ is odd.

But out corollary tells us that if $n = p_1^{r_1} \cdots p_m^{k_m}$ then

$$\tau(n) = (r_1 + 1)(r_2 + 1) \cdots (r_m + 1).$$

When is this product odd? Precisely when each factor is odd! This means that each r_j has to be even $r_j = 2s_j$, which translates to $n = \prod p_j^{2s_j} = \left(\prod p_j^{s_j}\right)^2$. The only switches which are "on" are the ones whose labels are perfect squares, for a total of $\lfloor \sqrt{2022} \rfloor = 44$.

□

Remark 4. For those students who were familiar with this question, I stated a variant where you only perform the flips for those d which are prime. Which light switches are "on" at the end? Arguing identically, it is precisely those $n = p_1^{r_1} \cdots p_m^{r_m}$ which are a multiple of an odd number of primes, i.e., if m is odd. Counting the number of n for which m is odd is still an open problem, but you are welcome to play around on a computer to estimate.

Lecture 7
2022-09-07

---

3 Modular arithmetic

This is chapter 2 in the textbook.

In dealing with gcds the most important tool at our disposal was division with remainder. The sequence of remainders decreased until the last nonzero remainder gave the gcd in the Euclidean algorithm. It turns out that focusing on these remainders will allow us to simplify enormously a lot of computations in number theory.

Definition 24. Suppose $n \geq 1$. We say that $a \equiv b \pmod{n}$ if a and b give the same remainder when divided by n.

Example 25. $2022 \equiv 22 \pmod{8}$ because both give remainder 6.

Remark 5. Because in division with remainder the remainder is always between 0 and $n-1$, any integer a is congruent modulo n to some $b \in \{0, 1, \ldots, n-1\}$. Whenever we write $a \mod n$ we mean precisely the b in this set.

The reason the notion of congruence is so useful is that it behaves well with respect to algebraic operations:

Proposition 26. *Suppose* $a \equiv b \pmod{n}$ *and* $a' \equiv b' \pmod{n}$. *Then* $a+a' \equiv b+b' \pmod{n}$ *and* $a \cdot a' \equiv b \cdot b' \pmod{n}$.

Proof. First, we need to switch perspectives from remainders to multiples of n. When we say $a \equiv b \pmod{n}$, i.e., that a and b give the same remainder when divided by n, we mean

$$a = nq_1 + r$$
$$b = nq_2 + r$$

so, subtracting, that $a - b = n(q_1 - q_2)$ is a multiple of n. Vice-versa, if $a - b$ is a multiple of n, then $a \equiv b \pmod{n}$.

So the two given congruences imply that $a = b + np$ and $a' = b' + nq$ for some integers p and q. Therefore

$$\begin{aligned} a + b &= a' + b' + n(p+q) & \qquad a + b &\equiv a' + b' \pmod{n} \\ ab &= (a'+np)(b'+nq) = a'b' + n(a'q + b'p + npq) & \qquad ab &\equiv a'b' \pmod{n}. \end{aligned}$$

□

Remark 6. An excellent way to keep this property in mind is that for any polynomial $P(X)$, we can compute $P(a) \mod n$ by evaluating $P(r) \mod n$, where $r = a \mod n$. Indeed, if $a \equiv r \pmod{n}$ then $a^d \equiv r^d \pmod{n}$ for each positive exponent d, so $P(a) \equiv P(r) \pmod{n}$.

Example 27. Let's work out some examples.

1. What kinds of remainders do perfect squares when dividing by 4? I.e., what is $P(x) = x^2 \mod 4$ if x is an integer? Because $P(x) \equiv P(x \mod 4) \pmod{4}$ by the remark, we really only ever need to worry about $x \mod 4 \in \{0, 1, 2, 3\}$. Then we can compute explicitly $0^2 \equiv 2^2 \equiv 0 \pmod{4}$ and $1^2 \equiv 3^2 \equiv 1 \pmod{4}$. Therefore perfect squares can only be $0, 1 \pmod{4}$.

   A beautiful consequence is that $x^2 + y^2 \mod 4$ can only be $0+0=0, 0+1=1+0=1, 1+1=2$ which means that NO integer $\equiv 3 \pmod{4}$ can ever be written as a sum of two perfect squares.

2. What kinds of remainders do we get when we evaluate $P(x) = x^3 + x + 1 \pmod{5}$? Again, we don't need to evaluate $P(x)$ for all integers x, but only $P(x \mod 5)$! But $x \mod 5 = 0, 1, 2, 3, 4$ and we can evaluate $P(0) \equiv P(2) \equiv P(3) \equiv 1 \pmod{5}$, $P(1) \equiv 3 \pmod{5}$ and $P(4) \equiv 4 \pmod{5}$. This means, for instance, that the integer $x^3 + x + 1$ can never end in the digit 7, as ending in the digit 7 means $\equiv 2 \pmod{5}$.

3. Sometimes it is helpful to reduce modular arithmetic computations differently. For instance, suppose we want to find all possible remainders of $P(x) = x^3$ when divided by 13. We don't need to do this for all integer x, but only for the possible values of $x \mod 13$, in other words, for $x \mod 13 \in \{0, 1, \ldots, 12\}$.

But because $1 + 12 = 2 + 10 = \ldots = 6 + 7 = 13$ it follows that

$$\begin{aligned} 12 &\equiv -1 \pmod{13} \\ 11 &\equiv -2 \pmod{13} \\ 10 &\equiv -3 \pmod{13} \\ 9 &\equiv -4 \pmod{13} \\ 8 &\equiv -5 \pmod{13} \\ 7 &\equiv -6 \pmod{13}, \end{aligned}$$

so really the possible values of $x \mod 13$ are $\pm 1, \pm 2, \ldots, \pm 6$. Why is this in any way better? That's because $P(-x) = (-x)^3 = -x^3$ so we can compute

$$\begin{aligned} P(1) \equiv P(12) \equiv P(\pm 1) \equiv \pm 1 \equiv 1, 12 \pmod{13} \\ P(2) \equiv P(11) \equiv P(\pm 2) \equiv \pm 8 \equiv 5, 8 \pmod{13} \\ P(3) \equiv P(10) \equiv P(\pm 3) \equiv \pm 27 \equiv \pm 1 \equiv 1, 12 \pmod{13} \\ P(4) \equiv P(9) \equiv P(\pm 4) \equiv \pm 64 \equiv \pm 12 \equiv 12, 1 \pmod{13} \\ P(5) \equiv P(8) \equiv P(\pm 5) \equiv \pm 125 \equiv \pm 8 \equiv 5, 8 \pmod{13} \\ P(6) \equiv P(7) \equiv P(\pm 6) \equiv \pm 216 \equiv \pm 8 \equiv 5, 8 \pmod{13}. \end{aligned}$$

4. What happens to the Fibonacci sequence modulo 3? We see that it repeats

$$\underbrace{0, 1, 1, 2, 0, 2, 2, 1}_{\text{repeats}}, 0, 1, 1, \ldots$$

Modulo 5? The same

$$\underbrace{0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1}_{\text{repeats}}, 0, 1, 1, \ldots$$

Is it the case that modulo any positive integer, the Fibonacci sequence repeats? Yes! The proof reveals something deep about the reason modular arithmetic is so useful.

Consider the tuple $(F_n \mod N, F_{n+1} \mod N)$. Since this is a tuple of remainders, with each entry in $0, 1, \ldots, N-1$, there are only N^2 possibilities that can occur. Therefore, once we enumerate more than N^2 consecutive terms, by the pigeonhole principle at least two such pairs must coincide. Say $(F_m, F_{m+1}) \equiv (F_n, F_{n+1}) \pmod{N}$. We'll show by induction that $F_{m+k} \equiv F_{n+k} \pmod{N}$ for all k, positive or negative. The base case is $k = 0, 1$. Suppose we know the congruence for k. Then (if $k > 1$)

$$F_{m+k+1} = F_{m+k} + F_{m+k-1} \equiv F_{n+k} + F_{n+k-1} = F_{n+k} \pmod{N}.$$

If $k < 0$ then

$$F_{m+k-1} = F_{m+k+1} - F_{m+k} \equiv F_{n+k+1} - F_{n+k} = F_{n+k-1} \pmod{N}.$$

Lecture 8
2022-09-09

3.1 Divisibility criteria

Two beautiful applications of modular arithmetic are the classical divisibility criteria with 3/9 and 11.

Proposition 28. *Suppose $N = a_d a_{d-1} \ldots a_1 a_0$ is a number written in base 10.*

1. $3 \mid N$ *(resp.* $9 \mid N$*) if and only if* $3 \mid a_0 + a_1 + \cdots + a_d$ *(resp.* $9 \mid a_0 + a_1 + \cdots + a_d$*).*

2. $11 \mid N$ *if and only if* $11 \mid a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^d a_d$*.*

Proof. Part (2) only, as the first one is identical.

We need a criterion for $N \equiv 0 \pmod{11}$. But $10 \equiv -1 \pmod{11}$ so

$$\begin{aligned} N &= a_d a_{d-1} \dots a_0 \\ &= a_d \cdot 10^d + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_d \cdot (-1)^d + \cdots + a_1 \cdot (-1) + a_0 \pmod{11}, \end{aligned}$$

so N is a multiple of 11 if and only if its alternating sum of digits is. □

Try your hands at the following similar statement, that we'll use later.

Problem 29. Suppose $N = a_d \dots a_1 a_{0(b)}$ is a positive integer written in base b, and let $s_b(N) = a_0 + \cdots + a_d$ the sum of its digits. Show that $\dfrac{N - s_b(N)}{b-1} \in \mathbb{Z}$.

Proof. This is equivalent to showing that $N - s_b(N)$ is a multiple of $b-1$, i.e., that $N \equiv s_b(N) \pmod{b-1}$. The rest of the argument is identical to that of Proposition 28. □

Example 30. What are all palindrome primes with an even number of digits?

Proof. An example? 11. We'll show this is the only one.

Any such prime will look like $a_1 a_2 \dots a_d a_d a_{d-1} \dots a_1$. Going through the divisibility criteria, the only plausible one is with 11. Indeed, computing the alternating sum of digits we get

$$a_1 - a_2 + \ldots + (-1)^d a_d + (-1)^{d+1} a_{d-1} + (-1)^{d+2} a_{d-2} + \ldots + (-1)^{d+d-1} a_1 = a_1 + (-1)a_1 - a_2 + (-1)^2 a_2 + \ldots + (-1)^d a_d + (-1)^{d-1} a_d =$$

Therefore any palindrome with an even number of digits must be a multiple of 11. Therefore 11 is the only prime with this property. □

3.2 Exponentiating mod n is fast

Exponentials a^b are huge, but however large they may be, computing $a^b \mod n$ is very fast.

Example 31. Say we want to compute $2^{123456789} \mod 123456789$.

Attempt 1: We could try to repeatedly multiply by 2:

$$\begin{aligned} 2 &= 2 \pmod{123456789} \\ 2^2 &= 4 \pmod{123456789} \\ 2^3 &= 8 \pmod{123456789} \\ 2^4 &= 16 \pmod{123456789} \\ &\vdots \end{aligned}$$

but this would take 123456789 operations.

Attempt 2: We could, instead, repeatedly square the previous answer:

$$\begin{aligned} 2 &= 2 \pmod{123456789} \\ 2^2 &= 4 \pmod{123456789} \\ 2^4 &= (2^2)^2 = 4^2 = 16 \pmod{123456789} \\ 2^8 &= (2^4)^2 = 16^2 = 256 \pmod{123456789} \\ &\vdots \\ 2^{2^{26}} &= (2^{2^{25}})^2 = 89107330^2 = 35687662. \end{aligned}$$

How could this possibly be enough? The reason is that we know how to write the desired exponent 123456789 in terms of powers of 2, namely by writing it in base 2:

$$123456789 = 111010110111100110100010101_{(2)} = 2^{26}+2^{25}+2^{24}+2^{22}+2^{20}+2^{19}+2^{17}+2^{16}+2^{15}+2^{14}+2^{11}+2^{10}+2^8+2^4+2^2+1.$$

This means that

$$\begin{aligned}
2^{123456789} &= 2^{2^{26}+2^{25}+2^{24}+2^{22}+2^{20}+2^{19}+2^{17}+2^{16}+2^{15}+2^{14}+2^{11}+2^{10}+2^8+2^4+2^2+1} \\
&= 2^{2^{26}} \cdot 2^{2^{25}} \cdot 2^{2^{24}} \cdot 2^{2^{22}} \cdot 2^{2^{20}} \cdot 2^{2^{19}} \cdot 2^{2^{17}} \cdot 2^{2^{16}} \cdot 2^{2^{15}} \cdot 2^{2^{14}} \cdot 2^{2^{11}} \cdot 2^{2^{10}} \cdot 2^{2^8} \cdot 2^{2^4} \cdot 2^{2^2} \cdot 2^1 \\
&\equiv 35687662 \cdots 16 \cdot 2 \pmod{123456789} \\
&\equiv 21492350 \pmod{123456789}.
\end{aligned}$$

3.3 The agebraic structure of the possible residues: the ring $\mathbb{Z}_n$

Until now, all remainders when dividing by n, also referred to as "residues mod n", were computationally obtained. In general, we need to understand their algebraic structure in order to make computations more conceptual.

Definition 32. Given an integer r, by $\overline{r}$ we mean the collection of all integer $\equiv r \pmod n$, i.e., $\overline{r} = \{\ldots, r-n, r, r+n, \ldots\}$. In particular, we see that $\overline{r} = \overline{r \pm n} = \overline{r \pm 2n} = \ldots$ and, given a set S of this form, the choice of an integer r such that $S = \overline{r}$ is called a **representative**. Vice-versa, if $\overline{x} = \overline{y}$ then $x \equiv y \pmod n$.

We then denote $\mathbb{Z}_n$ the set $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ of all possible residues mod n.

Remark 7. By Proposition 26, $\overline{x} + \overline{y} = \overline{x+y} = \overline{x+y \mod n}$ and $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{xy \mod n}$.

Lecture 9
2022-09-12

A huge **goal** for us will be to understand the structure of $\mathbb{Z}_n$ with respect to these algebraic operations, addition and multiplication, which turn it into a "ring".

1. Is $\mathbb{Z}_n$ a field? (Yes, if n is a prime.)
2. Does multiplication have an inverse in general? (Yes, on the unit group.)
3. We know operations repeat in $\mathbb{Z}_n$, but how soon? (For multiplication, it's the multiplicative order.)
4. Does $\mathbb{Z}_n$ have a predictable structure? (Yes, given by the Chinese Remainder Theorem.)
5. Does the unit group $\mathbb{Z}_n^\times$ have a predictable structure? (Yes, given by the Chinese Remainder Theorem and cyclicity results.)

3.4 Invertibility mod n

We begin with the question of invertibility. Let's start with the familiar setting of integers. What does it mean that an integer x has an inverse x^{-1}? This question can have two meanings, and therefore two answers:

1. For what integers x is there a meaningful notion of x^{-1}? In this case the answer is $x \neq 0$, as in that case $x^{-1} = \frac{1}{x}$ is a meaningful rational number.
2. For what integers x is there a notion of x^{-1} without reference to any other ambient space other than the integers. In other words, x^{-1} is also an integer. The answer to this question is $x \in \{-1, 1\}$, as a product of integers $x \cdot x^{-1} = 1$ can only occur in the case $1 \cdot 1 = 1$ or $-1 \cdot -1 = 1$.

It is the latter notion that makes sense for $\mathbb{Z}_n$: we say that $a \in \mathbb{Z}_n$ is invertible if there exists $a^{-1} \in \mathbb{Z}_n$.

Lemma 33. *Suppose $a \in \mathbb{Z}$ is a representative of a class $a \in \mathbb{Z}_n$ (abuse of notation). Then $a^{-1} \in \mathbb{Z}_n$ exists if and only if $(a, n) = 1$.*

Proof. What does it mean for a^{-1} to exist? It means that we can find some integer b ($b \equiv a^{-1} \pmod{n}$) such that $a \cdot b = \overline{1} \in \mathbb{Z}_n$, i.e., that $a \cdot b \equiv 1 \pmod{n}$ so $a \cdot b = 1 + nd$. This means that $ab - nd = 1$. But we already know, from Proposition 18 that such integers exist if and only if $(a, n) \mid 1$, i.e., a and n are coprime. □

Remark 8. The proof above gives a recipe for computing $a^{-1} \pmod{n}$ using Bézout.

Example 34. Compute $3^{-1} \pmod{11}$. Here we can guess: since $3 \cdot 4 = 12$ we see that $4 \equiv 3^{-1} \pmod{11}$.

Problem 35. For Halloween you bought a number of bags of 15 candies each. You decide to treat big kids and small kids differently. You make the following observations:

1. If you try to give small kids 7 candies each and big kids 3 candies each, you are 2 candies short.
2. If you try to give small kids 3 candies each and big kids 5 candies each, you are 8 candies short.

What's the smallest number of kids that can fit your observations?

Proof. Let x be the number of small kids, y the number of big kids, and z the number of bags of candies. In the first setting, you need $7x + 3y$ candies, but you are 2 short, so $7x + 3y = 2 + 15z$. In the second setting, you need $3x + 5y$ candies, but you are 8 short, so $3x + 5y = 8 + 15z$. Using the language of congruences modulo 15, we need to solve for $x, y \in \mathbb{Z}_{15}$ the system:

$$\begin{aligned} 7x + 3y &\equiv 2 \pmod{15} \\ 3x + 5y &\equiv 8 \pmod{15}. \end{aligned}$$

We can substitute one variable for the other. From the first one, we can't really compute y in terms of x as 3 is NOT invertible modulo 15, but $7^{-1} \equiv -2 \equiv \pmod{15}$ so $x \equiv 7^{-1}(2 - 3y) \equiv -2(2 - 3y) \equiv 6y - 4 \pmod{15}$. Substituting into the second equation we get that $3x+5y \equiv 3(6y-4)+5y \equiv 23y-12 \equiv 8y-12 \equiv 8 \pmod{15}$ which can be solved as $y \equiv 5 \cdot 8^{-1} \equiv 10 \pmod{15}$ and therefore $x \equiv 11 \pmod{15}$. Alternatively, we could use linear algebra:

$$\begin{aligned} \begin{pmatrix} 7 & 3 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &\equiv \begin{pmatrix} 2 \\ 8 \end{pmatrix} \pmod{15} \\ \begin{pmatrix} x \\ y \end{pmatrix} &\equiv \begin{pmatrix} 7 & 3 \\ 3 & 5 \end{pmatrix}^{-1} \begin{pmatrix} 2 \\ 8 \end{pmatrix} \\ &\equiv 26^{-1} \begin{pmatrix} 5 & -3 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} 2 \\ 8 \end{pmatrix} \\ &\equiv \begin{pmatrix} 13 & 6 \\ 6 & 4 \end{pmatrix} \begin{pmatrix} 2 \\ 8 \end{pmatrix} \\ &\equiv \begin{pmatrix} 11 \\ 10 \end{pmatrix} \pmod{15}. \end{aligned}$$

As $x \equiv 11 \pmod{15}$ and $y \equiv 10 \pmod{15}$, the smallest possible number of kids is $x + y = 11 + 10 = 21$. □

3.5 The Chinese Remainder Theorem

The Chinese Remainder Theorem, one of the few appropriately named theorems of math, describes $\mathbb{Z}_n$ in simpler terms.

Theorem 36 (CRT)**.** *Suppose m and n are positive coprime integers. Then the map $x \mod mn \mapsto (x \mod m, x \mod n)$ gives a bijection*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n,$$

which respects $+$ and $\cdot$.

Example 37. What is the last digit of 2^{1000}? In other words, what is $2^{1000} \mod 10$? The CRT tells us that knowing the answer $\mod 10$ is equivalent to knowing the answer $\mod 2$ and $\mod 5$.

$$\begin{aligned} 2^{1000} &= 0 \pmod 2 \\ 2^{1000} &= (2^2)^{500} = 4^{500} \\ &\equiv (-1)^{500} = 1 \pmod 5. \end{aligned}$$

Therefore $2^{1000} \mod 10$, a priori a digit in $\{0, 1, \ldots, 9\}$, must be $\equiv 0 \pmod 2$ (so in $\{0, 2, 4, 6, 8\}$) and $\equiv 1 \pmod 5$ (so in $\{1, 6\}$). By inspection, the only possibility is 6.

Lecture 10
2022-09-14

The proof of Theorem 36 below will be constructive, which is essential for computations.

Proof of CRT. Let's look at the assignment $x \mod mn \mapsto (x \mod m, x \mod n)$ from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m \times \mathbb{Z}_n$. We need to show

1. it is well-defined. After all, $x \mod N$ depends on x, but we don't start with an integer x on the left, instead we start with $x \mod mn$. We need to make sure that on the right we get a pair which doesn't depend on the integer x, but only on the residue $x \mod mn$. What if $x \equiv y \pmod{mn}$ and we try to use y instead of x. In this case $y = x + mnd$ for some integer d, so $y \equiv \pmod m$ and $y \equiv \pmod n$. This means that the answer on the right doesn't change if we use y instead of x so the assignment is a well-defined function.
2. it respects $+$ and $\cdot$. This is fine, because we know that $x \mod N + y \mod N = (x + y) \mod N$.
3. the function is injective.
4. the function is surjective.

We'll treat the last 2 separately. Suppose $x \mod mn$ and $y \mod mn$ are residue classes such that

$$(x \mod m, x \mod n) = (y \mod m, y \mod n).$$

This means that $x \equiv y \pmod m$ and $x \equiv y \pmod n$ so $x - y$ is a multiple of m and n. Now we use that m and n are coprime! Because of this, a multiple of m and n is the same thing as a multiple of mn. Therefore $x \equiv y \pmod{mn}$ so $x \mod mn = y \mod mn$, in other words, the function is injective.

Finally, we get to surjectivity, where again we use that m and n are coprime, this time in the guise of Bézout's formula. As $(m, n) = 1$, we can find two integers u and v such that $mu + nv = 1$. We need to show that for any $a \mod m \in \mathbb{Z}_m$ and $b \mod n \in \mathbb{Z}_n$, we can find $x \mod mn$ such that

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n. \end{aligned}$$

Let's try out $x = anv + bmu$. (Careful with the ordering: a is paired with nv NOT mu.) I claim this works. Indeed,

$$\begin{aligned} x &= anv + bmu \\ &\equiv anv \pmod m \\ &\equiv a(1 - mu) \pmod m \\ &\equiv a \pmod m, \end{aligned}$$

and similarly for $x \equiv b \pmod{n}$.

□

Remark 9. The hypothesis that m and n are coprime is used for both injectivity and surjectivity. This makes sense because both $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have the same number of elements, namely mn. The pigeonhole principle implies that a function between two sets of the same finite cardinality is injective if and only if it is surjective. In particular, we needn't have worked out surjectivity separately, as it is a consequence of injectivity. However, our proof is constructive, which is something we need to be able to do anyway.

CRT has both fun and extremely useful applications, but let's start with the fun.

Problem 38 (Putnam 1955)**.** Show that for any n, you can find n consecutive integers such that none of them is square-free.

Proof. We seek $x+1, x+2, \ldots, x+n$ none of which is square-free. There's an easy way to guarantee that an integer is not square-free, namely make it a multiple of some p^2. That's what we'll do: choose distinct arbitrary primes $p_1, \ldots, p_n$ and seek x such that $x+i$ is a multiple of p_i^2. In other words, $x \equiv -i \pmod{p_i^2}$. This is possible by CRT. □

Problem 39 (IMO 1989)**.** Prove that for each positive integer n there exist n consecutive positive integers none of which is an integral power of a prime number.

Proof. Same proof as above, but with $x + i \equiv 0 \pmod{p_i q_i}$. □

Problem 40. A positive integer has the same last 2 digits as its square. What are these last 2 digits?

Proof. We seek $N \mod 100$ such that $N^2 \equiv N \pmod{100}$. By CRT it's enough that $N^2 \equiv N \pmod 4$ and $N^2 \equiv N \pmod{25}$. For the former, we could enumerate, and see that only $N \equiv 0, 1 \pmod 4$ work. For the later enumeration is more laborious. In general, if $N^2 \equiv N \pmod{p^k}$ for a prime power p^k then $N^2 - N = N(N-1) \equiv 0 \pmod{p^k}$ so $p^k \mid N(N-1)$. Since N and $N-1$ are coprime, either $p^k \mid N$ or $p^k \mid N-1$ so in general $N \equiv 0, 1 \pmod{p^k}$. Therefore $N \equiv 0, 1 \pmod{25}$. Using CRT to find $N \mod 100$ we get the following last two digits:

	$N \equiv 0 \pmod{25}$	$N \equiv 1 \pmod{25}$
$N \equiv 0 \pmod 4$	00	76
$N \equiv 1 \pmod 4$	25	01

□

Problem 41. The discriminant of the cubic polynomial $X^3 + aX + b$ is $\Delta = -4a^3 - 27b^2$. Show that for every integer n you can find integers a, b, not both multiples of n, such that Δ is a multiple of n.

Proof. It's enough to show this modulo prime powers, where we seek a, b not both $\equiv 0 \pmod{p^k}$, such that $\Delta \equiv 0 \pmod{p^k}$. Mod 2^k we can take $a = 2^{k-1}$ and $b = 0$. Mod 3^M we can take $a = 0$ and $b = 3^{k-1}$. Mod p^k for $p > 3$ we can take $b \equiv 2 \pmod{p^k}$ and try to solve for a: $-4a^3 \equiv 4 \cdot 27 \pmod{p^k}$ so $a \equiv 3 \pmod{p^k}$ works. □

Lecture 11
2022-09-16

3.6 The Euler function

One of the most useful applications of CRT is to the computation of the Euler function $\varphi(n) = |\mathbb{Z}_n^\times|$.

Theorem 42. *We have*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Lemma 43. *If m and n are coprime then the CRT map $x \mod mn \mapsto (x \mod m, x \mod n)$ gives a bijection*

$$\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times.$$

Proof. If $x \mod mn$ is invertible modulo mn then x must be coprime to mn, which means x must be coprime to m and x must be coprime to n. Therefore, $x \mod m$ is invertible and $x \mod n$ is invertible. In the other direction, $x \mod m$ (resp. $x \mod n$) is invertible means x is coprime to m (resp. n) and therefore x must be coprime to mn. □

Corollary 44. *By definition, if m and n are coprime,*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proof of Theorem 42. Let's first show that $\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$. We are counting integers $1 \le a \le p^k$ which are coprime to p. From the total of p^k we must eliminate the p^{k-1} which are multiples of p, yielding the desired formula.

Factor $n = p_1^{k_1} \cdots p_r^{k_r}$. By the corollary,

$$\begin{aligned}\varphi(n) &= \prod \varphi(p_i^{k_i}) \\ &= \prod p_i^{k_i}\left(1 - \frac{1}{p_i}\right) \\ &= n\prod_{p|n}\left(1 - \frac{1}{p}\right).\end{aligned}$$

□

The Euler function is very useful because of the following major result:

Theorem 45. *If a is coprime to n then $a^{\varphi(n)} \equiv 1 \pmod n$. When $n = p$ is a prime, we recover Fermat's little theorem $a^{p-1} \equiv 1 \pmod p$ whenever a is not a multiple of p.*

Proof. The proof relies on the following observation: if a and x are coprime to n, then so is ax. This means that we get a multiplication map $\mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ sending $f : \overline{x} \mapsto \overline{ax}$. This map is surjective: indeed, as $(a, n) = 1$ it follows that $\overline{a}^{-1} \in \mathbb{Z}_n^\times$ so $f(\overline{a}^{-1}\overline{x}) = \overline{x}$. Moreover, it is injective: if $f(x) = f(y)$ then $\overline{ax} = \overline{ay}$ so, multiplying with $\overline{a}^{-1}$ we get $\overline{x} = \overline{y}$.

This means that $\mathbb{Z}_n^\times = \operatorname{Im} f = \{\overline{a} \cdot \overline{x} \mid \overline{x} \in \mathbb{Z}_n^\times\}$. For instance,

$$\mathbb{Z}_{15}^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

and

$$7\mathbb{Z}_{15}^\times = \{\overline{7}, \overline{14}, \overline{13}, \overline{4}, \overline{11}, \overline{2}, \overline{1}, \overline{8}\}.$$

We see that $a\mathbb{Z}_n^\times$ is a permutation of $\mathbb{Z}_n^\times$. This permutation can be arbitrary, but the product of the elements is independent of the ordering so

$$\prod_{\overline{x} \in \mathbb{Z}_n^\times} \overline{x} = \prod_{\overline{x} \in \mathbb{Z}_n^\times} \overline{ax} = \overline{a}^{\varphi(n)} \prod_{\overline{x} \in \mathbb{Z}_n^\times} \overline{x}.$$

The product is a product of invertible elements and therefore must also be invertible, so we can cancel it on both sides and get $\overline{a}^{\varphi(n)} = \overline{1}$, in other words $a^{\varphi(n)} \equiv 1 \pmod n$. □

A beautiful and very useful application is the following:

Problem 46. Suppose $m, n \in \mathbb{Z}$ and p is a prime such that $p \mid m^2 + n^2$. If $p \equiv 3 \pmod 4$ then $p \mid m$ and $p \mid n$.

Proof. Suppose $p \nmid m, n$. Then $m^2 + n^2 \equiv 0 \pmod{p}$ becomes $-1 \equiv (m/n)^2 \pmod{p}$. If $p = 4k + 3$ then $p - 1 = 4k + 2$ so

$$1 \equiv (m/n)^{p-1} \equiv (m/n)^{4k+2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

which is impossible, as $1 \equiv -1 \pmod{p}$ only holds if $p = 2$. □

Corollary 47. *If $(a, n) = 1$ then $a^N \equiv a^{N \bmod \varphi(n)} \pmod{n}$.*

Example 48. Compute $2^{3^{4^5}} \bmod 90$.

Proof. The exponent here is huge, it has 489 digits and $90 = 2 \cdot 3^2 \cdot 5$ (the modulus) is quite large, too. Let's, instead, use CRT, to compute $2^{3^{4^5}}$ modulo 2, 3^2, and 5. First, mod 2 we get 0. Mod 3^2 we use $\varphi(9) = 6$ so

$$2^{3^{4^5}} \equiv 2^{3^{4^5} \bmod 6} \pmod{9}.$$

For the exponent we'll use CRT again. Mod 2, $3^{4^5} \equiv 1 \pmod{2}$ (odd!). Mod 3 it is clearly 0. CRT then tells us that $3^{4^5} \equiv 3 \pmod{6}$ so

$$2^{3^{4^5}} \equiv 2^{3^{4^5} \bmod 6} \equiv 2^3 \equiv -1 \pmod{9}.$$

Mod 5, with $\varphi(5) = 4$, the corollary gives

$$2^{3^{4^5}} \equiv 2^{3^{4^5} \bmod 4} \equiv 2^{(-1)^{4^5} \bmod 4} \equiv 2 \pmod{5}.$$

Let's use explicit CRT to put everything together: $2 \cdot 5 + 9 \cdot (-1) = 1$ so our number is $\equiv 0 \cdot (-9) + (-1) \cdot 10 \equiv -10 \equiv 8 \pmod{18}$. Then $18 \cdot 2 + 5 \cdot (-7) = 1$ so our number is $\equiv 8 \cdot (-35) + 2 \cdot 36 \equiv -208 \equiv 62 \pmod{90}$. □

While such exponentiation examples are fun, the real use of the corollary comes in its application to solving cryptographic equations:

Proposition 49. *Let a be coprime to n and e be coprime to $\varphi(n)$. Then the equation*

$$x^e \equiv a \pmod{n}$$

has a **unique** *solution $x \equiv a^f \pmod{n}$ where $f \equiv e^{-1} \pmod{\varphi(n)}$.*

Proof. We can't quite show uniqueness yet, as that is a consequence of the cyclic structure of $\mathbb{Z}_{p^k}^\times$, but we can check that it is a solution. Indeed,

$$x^e \equiv (a^f)^e \equiv a^{ef} \equiv a^{ef \bmod \varphi(n)} \equiv a \pmod{n}.$$

□

Example 50. Find an x such that $x^{17} \equiv 23 \pmod{123}$. Here $\varphi(123) = 80$ and $17^{-1} \equiv 33 \pmod{80}$ so

$$x \equiv \text{“}\sqrt[17]{23}\text{”} \pmod{123} \equiv \text{“}23^{17^{-1}}\text{”} \pmod{123} \equiv 23^{17^{-1} \bmod 80} \pmod{123} \equiv 23^{33} \equiv 113 \pmod{123}.$$

Lecture 12
2022-09-19

3.7 Multiplicative order

We saw that if a and n are coprime, then always

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Definition 51. The multiplicative order of a mod n is the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

Remark 10. The multiplicative order of a always exists if a is coprime to n, and never exists when a is not coprime to n. Indeed, if $a^d \equiv 1 \pmod{n}$ then $a^{-1} \equiv a^{d-1} \pmod{n}$ so a must be coprime to n.

Example 52. The order of -1 is always 2, the order of $2 \mod 17$ is 8.

How does one check what the multiplicative order is? The last thing to do is to check every exponent $a, a^2, a^3, \ldots$ until one arrives at $\equiv 1 \pmod{n}$.

Lemma 53. *Suppose a and n are coprime. Then*

1. $\operatorname{ord}(a)$ *divides any integer D such that $a^D \equiv 1 \pmod{n}$. In particular,* $\operatorname{ord}(a) \mid \varphi(n)$.
2. *To verify that* $\operatorname{ord}(a) = d$ *it is enough to check that*
   (a) $a^d \equiv 1 \pmod{n}$ *and*
   (b) $a^{d/q} \not\equiv 1 \pmod{n}$ *for any* **prime** $q \mid d$.

Proof. (1) Suppose $\operatorname{ord}(a) = d \nmid D$. Divide with remainder and get $D = dq + r$ where $0 < r < D$. But then

$$a^r = a^{D-dq} = a^D \cdot (a^d)^{-q} \equiv 1 \pmod{n}$$

contradicting the fact that d is the smallest positive exponent which gives $\equiv 1 \pmod{n}$.

(2) Suppose $a^d \equiv 1 \pmod{n}$ but $\operatorname{ord}(a) \neq d$. From the first part, $\operatorname{ord}(a) \mid d$ and, because the two numbers are not equal, $d/\operatorname{ord}(a) > 1$ must have a prime divisor q. Then $\operatorname{ord}(a) \mid d/q$ so $a^{d/q} \equiv 1 \pmod{n}$, a contradiction. □

Problem 54. Compute the decimal expansion of $\frac{3}{84}$. Compute the decimal expansion of $\frac{1}{7}$ in base 5.

Proof. (1) We begin with factoring the denominator into a part coprime to 10, and a part involving only powers of 2 or 5.

$$\begin{aligned}\frac{3}{84} &= \frac{3}{4 \cdot 21} \\ &= \frac{3 \cdot 25}{100 \cdot 21}.\end{aligned}$$

Next, 21 being coprime to 10, we find the multiplicative order of 10 modulo 21. Since $\varphi(21) = 12$, we need to verify exponents $10^{12/2} \equiv 1 \pmod{21}$ and $10^{12/3} \equiv 4 \pmod{21}$. We see that $\operatorname{ord}(10 \mod 21) \mid 6$ and check again $10^{6/2} \equiv 13 \pmod{21}$ and $10^{6/3} \equiv 16 \pmod{21}$. So the order is 6 and indeed $10^6 - 1 = 21 \cdot 47619$. We get

$$\begin{aligned}\frac{3}{84} &= \frac{75}{100 \cdot 21} \\ &= \frac{75 \cdot 47619}{100 \cdot (10^6 - 1)} \\ &= \frac{3619044}{100 \cdot 999999} \\ &= \frac{1}{100} \cdot \left(3 + \frac{619047}{999999}\right) \\ &= 0.01 \cdot (3 + 0.\overline{619047}) \\ &= 0.03\overline{619047}.\end{aligned}$$

(2) The multiplicative order of 5 modulo 7 is 6 and $5^6 - 1 = 7 \cdot 2232$. So

$$\begin{aligned}\frac{1}{7} &= \frac{2232}{5^6 - 1} \\ &= \frac{32412_{(5)}}{444444_{(5)}} \\ &= 0.\overline{032412}_{(5)}.\end{aligned}$$

□

3.8 Primitive roots modulo p

The principal way in which the multiplicative order appears in theoretically imporant ways is via the group structure of $\mathbb{Z}_p^\times$.

We'll be working modulo a prime p. By Lemma 53, $\text{ord}(a) \mid p-1$ and we have an algorithmic criterion for computing $\text{ord}(a)$ exactly by enumerating the divisors of $p-1$. This enumeration can be problematic, from a computation point of view, when p is large. For instance, already for primes with 50 digits, Sage isn't able to factor $p-1$. The following theorem is about how large $\text{ord}(a)$ can be.

Theorem 55. *There exist* **primitive roots modulo** p*, i.e.,* $a \in \mathbb{Z}_p^\times$ *with order* $\text{ord}(a) = p-1$.

Example 56. We can compute $\text{ord}(2 \mod 11) = 10$ so 2 is a primitive modulo 11, but $\text{ord}(2 \mod 7) = 3$ so 2 is NOT a primitive root mod 7. However, 3 is a primitive root mod 7.

Remark 11. The reason primitive roots are crucial is that they allow us to use calculus methods in modular arithmetic. For instance, we note that $\mathbb{Z}_7^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\} = \{\overline{1}, \overline{3}, \overline{3}^2, \overline{3}^3, \overline{3}^4, \overline{3}^5\}$.

In general, if a is a primitive root modulo p then all the powers $\{\overline{1}, a, a^2, \ldots, a^{p-2}\}$ are distinct modulo p. Indeed, if $a^i \equiv a^j \pmod p$ for some $i > j$ then $a^{i-j} \equiv 1 \pmod p$. In this case, Lemma 53 implies that $p - 1 = \text{ord}(a) \mid i - j$, which is impossible as $i - j \{1, 2, \ldots, p-2\}$. Thus these $p-1$ powers of a are $p-1$ distinct elements of the set $\mathbb{Z}_p^\times$, which has $p-1$ elements. In conclusion:

$$\mathbb{Z}_p^\times = \{\overline{1}, a, a^2, \ldots, a^{p-2}\},$$

and powers of a give a permutation of $\mathbb{Z}_p^\times$.

Since every element of $\mathbb{Z}_p^\times$ is a power of a, we can always solve the equation $a^x \equiv b \pmod p$, and the solution $x =$ "$\log_a b$" $\mod p$ is called the "discrete logarithm". Computationally, discrete logarithms are hard, in the sense that there is no known fast algorithm for computing x in terms of a, b, p.

This computational difficulty makes primitive roots very useful for cryptography.

Some **big questions** about primitive roots:

1. How do we find primitive roots modulo p? Goes hand in hand with:
2. How many primitive roots modulo p are there? If there are many, we could randomly choose a and hope a works.
3. How often does 2 work as a primitive root? How about 3? Or 4?

The following classical application is inspired by Gauss' construction, with ruler and compass, of the regular 17-gon, which saw the introduction of so-called Gauss sums. These Gauss sums later led to quadratic reciprocity.

Problem 57. Let p be a prime. Consider the function $f(n) = 1^n + 2^n + \cdots + (p-1)^n$. For what positive integers n is $f(n)$ a multiple of p?

Proof. Let's compute some values.

$$f(1) = 1 + 2 + \cdots + (p-1) = \frac{p(p-1)}{2}$$
$$f(2) = 1^2 + 2^2 + \cdots + (p-1)^2 = \frac{p(p-1)(2p-1)}{6}$$
$$f(3) = 1^3 + 2^3 + \cdots + (p-1)^3 = (1 + 2 + \cdots + (p-1))^2 = f(1)^2.$$

We see that $p \mid f(1), f(3)$ whenever $p > 2$ and $p \mid f(2)$ whenever $p > 3$. It seems hard to guess.

We'll prove that $p \mid f(n)$ if and only if $p - 1 \nmid n$.

The idea is to compute $f(n) \pmod p$ in which case

$$f(n) \equiv \sum_{x \in \{1,2,\ldots,p-1\}} x^n = \sum_{x \in \mathbb{Z}_p^\times} x^n,$$

and we can use primitive roots modulo p. Theorem 56 implies that

$$\mathbb{Z}_p^\times = \{1, a, a^2, \ldots, a^{p-2}\}$$

so we can rewrite the sum over $x \in \{1, 2, \ldots, p-1\}$ as a sum over $x = a^k \in \{1, a, a^2, \ldots, a^{p-2}\}$.

$$\begin{aligned} f(n) &= \sum_{k=0}^{p-2} (a^k)^n \\ &= \sum_{k=0}^{p-2} (a^n)^k. \end{aligned}$$

If $p - 1 = \operatorname{ord}(a) \mid n$ then $a^n \equiv 1 \pmod p$ and therefore

$$f(n) \equiv \sum_{k=0}^{p-1} 1^k \equiv p - 1 \equiv -1 \pmod p.$$

If $p - 1 = \operatorname{ord}(a) \nmid n$ then, by Lemma 53, $y = a^n \not\equiv 1 \pmod p$. We can therefore apply the geometric series formula $1 + y + y^2 + \cdots + y^{p-2} = \frac{1-y^{p-1}}{1-y}$. But $y^{p-1} = (a^n)^{p-1} \equiv (a^{p-1})^n \equiv 1 \pmod n$ so

$$f(n) = \sum_{k=0}^{p-2} (a^n)^k \equiv \frac{1 - (a^n)^{p-1}}{1 - a^n} \equiv \frac{0}{1 - a^n} \equiv 0 \pmod p,$$

which makes sense as the denominator $1 - a^n$ is invertible modulo p, since it is nonzero. □

Lecture 13
2022-09-21

Let's see some more examples.

Problem 58. Previously, we found a solution to $x^{17} \equiv 23 \pmod{123}$. Let's show that this equation has a unique solution.

Proof. By CRT this is equivalent to showing that $x^{17} \equiv 23$ has a unique solution modulo 2 and 41. Modulo 2 it's easy, the only solution being 1. What about modulo 41? Let a be a primitive root modulo 41, i.e., $\operatorname{ord}(a) = 40$. Then we can write $x = a^y$ and $23 = a^m$. We now have to show that the equation $a^{17y} = a^m \pmod{41}$ has a unique solution. We don't need to solve it, only show that it has a single solution. In fact, we couldn't really solve it, as we don't know m, which is the discrete logarithm of 23 mod 41.

The equation $a^{17y} \equiv a^m \pmod{41}$ becomes $a^{17y-m} \equiv 1 \pmod{41}$. But Lemma 53 implies that this can only happen if $40 = \operatorname{ord}(a)$ divides the exponent $17y - m$, i.e., $17y \equiv m \pmod{40}$. This equation has a single solution, namely, $y \equiv 17^{-1}m \pmod{40}$. □

Let's return to the theorem on primitive roots. The textbook has a fantastic proof, which I recommend you read. We will, instead, prove a stronger version, using a different method. All proofs I am aware of begin with the following two observations:

Remark 12. Suppose p is a prime number.

1. $\mathbb{Z}_p$ is a field, as every nonzero element is invertible, in $\mathbb{Z}_p^\times = \mathbb{Z}_p - \{0\}$.
2. A polynomial of degree d with coefficients in a field can have at most d roots in that field.

We will apply the above observations to the polynomial $X^{p-1} - 1$ with coefficients modulo p.

Lemma 59. *We have*

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod{p}.$$

Moreover, if $m \mid p-1$, then $X^m - 1$ has exactly m roots in $\mathbb{Z}_p$.

Proof. By Fermat's little theorem, $1, 2, \ldots, p-1$ are roots of $X^{p-1} - 1$ modulo p. Since this polynomial can't have any more roots as $\mathbb{Z}_p$ is a field, the factorization above is true.

If $m \mid p-1$ then we saw before that $X^m - 1 \mid X^{p-1} - 1$ so $X^m - 1$ modulo p must divide $(X-1)(X-2)\cdots(X-(p-1))$ which means that the roots of $X^m - 1$ are in fact m elements in the set $\{1, 2, \ldots, p-1\}$. □

Corollary 60 (Wilson's theorem)**.** *If p is a prime then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Plug in 0 into Lemma 59.

□

Lecture 14
2022-09-23

We are now ready for (a stronger version of) the theorem on primitive roots.

Theorem 61. *Let p be a prime. Then there exist exactly $\varphi(p-1)$ primitive roots modulo p.*

Proof. This proof uses the language of probabilities. However, the only input will be the following fact:

> **Black box from probability:** Suppose $A_1, \ldots, A_n$ is a collection of mutually independent statements, i.e., $\Pr(A_{i_1} \& \ldots \& A_{i_k}) = \Pr(A_{i_1}) \cdots \Pr(A_{i_k})$. Then the negations of these statements are also mutually independent.

By Lemma 53 we know that if $a \in \mathbb{Z}_p^\times$ we can check whether a is a primitive root by verifying that $a^{p-1} \equiv 1 \pmod{p}$ (automatic from Fermat's little theorem) and $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all $q \mid p-1$.

For each $q \mid p-1$ let A_q be the statement "x is a root of $X^{(p-1)/q} - 1$ modulo p. By Lemma 59 this polynomial has $(p-1)/q$ distinct roots in $\mathbb{Z}_p^\times$ so $\Pr(A_q) = \frac{1}{q}$. Let's check that if $q_1, \ldots, q_k$ are distinct prime factors of $p-1$ then $A_{q_1}, \ldots, A_{q_k}$ are uncorrelated. In other words, we need to check that

$$\Pr(A_{q_1} \& \ldots \& A_{q_k}) = \prod \frac{1}{q_j}.$$

But the LHS counts the number of $x \in \mathbb{Z}_p^\times$ which are roots of $X^{(p-1)/q_1} - 1$, …, $X^{(p-1)/q_k} - 1$. How does one count common roots of a collection of polynomials? Simply count the roots of the gcd. We already saw that $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$, and the same holds for powers of X. This means that the roots common to all $X^{(p-1)/q_j} - 1$ are precisely the roots of $X^{(\frac{p-1}{q_1}, \frac{p-1}{q_2}, \ldots, \frac{p-1}{q_k})} - 1 = X^{\frac{p-1}{q_1 \cdots q_k}} - 1$. Again by Lemma 59 this has precisely $\frac{p-1}{\prod q_j}$ roots, so the probability statement above holds.

Let's now compute the probability that a random $x \in \mathbb{Z}_p^\times$ is a primitive root. Suppose now that $p_1, \dots, p_s$ are all the distinct prime factors of $p-1$. Then the above statement implies that

$$\begin{aligned}\Pr(x \in \mathbb{Z}_p^\times \text{ is primitive root}) &= \Pr(\text{not } A_{p_1} \& \dots \& \text{ not } A_{p_s}) \\ &= \prod \Pr(\text{not } A_{p_j}) \\ &= \prod \left(1 - \frac{1}{p_i}\right).\end{aligned}$$

We deduce that there are precisely $(p-1)\prod\left(1-\frac{1}{p_i}\right) = \varphi(p-1)$ primitive roots modulo p. □

Remark 13. The theorem implies that if p is a prime, we can choose randomly any $a \in \mathbb{Z}_p^\times$ and, with probability $\frac{\varphi(p-1)}{p-1}$, it will be a primitive root modulo p. This can be checked easily as long as we know the factorization of $p-1$.

I DIDN'T COVER THE REMAINDER OF THIS LECTURE'S NOTES DURING CLASS.

An altogether different question is whether we can simply use 2, or 3, or 4, or 5, etc as a primitive root modulo p. First, note that a perfect square can never be a primitive root mod p. The answer is no, as $(n^2)^{(p-1)/2} \equiv 1 \pmod p$.

In general, an answer is given by Artin's conjecture:

Problem 62. How often is 2 a primitive root modulo p? The probability is

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0.3739.$$

How often is 2 or 3 a primitive root? Etc. If we know the factorization of $p-1$ we can simply enumerate $2, 3, \dots$, skipping perfect squares, and check if we get a primitive root.

Proof. This is not a proof per se, only a heuristic. The first probability is known if one assumes the Generalized Riemann Hypothesis.

To check whether 2 is a primitive root we require that $2^{p-1} \equiv 1 \pmod p$ (automatic) and $2^{(p-1)/q} \not\equiv \pmod p$ for every $q \mid p-1$. This means that

$$\Pr(2 \text{ is a primitive root mod } p) = \Pr(2^{(p-1)/q} \not\equiv 1 \pmod p \text{ for all } q \mid p-1).$$

We now execute a heuristic leap of faith, asserting that in the formula the events on the RHS are independent as q varies among all primes. Given a prime q, what is the probability that $2^{(p-1)/q} \not\equiv 1 \pmod p$ for $q \mid p-1$? This equals $1 - \Pr(q \mid p-1 \& 2^{(p-1)/q} \equiv 1 \pmod p)$ and therefore

$$\Pr(2 \text{ is a primitive root mod } p) = \prod_{q \text{ prime}} \left(1 - \Pr(p \equiv 1 \pmod q \& 2^{(p-1)/q} \equiv 1 \pmod p)\right).$$

Now $p \mod q$ has $q-1$ possible values (since $q \nmid p$, $p \mod q \in \mathbb{Z}_q^\times$), and the probability that it is 1 is $\frac{1}{q}$ (Dirichlet's theorem, for later). Similarly, $2^{(p-1)/q}$ is a root of the polynomial $X^q - 1 \mod p$, which has exactly q roots in $\mathbb{Z}_p^\times$. We impose the assumption that this root is random among the q roots of $X^q - 1$, and therefore it is precisely the root 1 with probability $\frac{1}{q}$. Again, we impose the assumption that the two congruences are uncorrelated, which means that $\Pr(p \equiv 1 \pmod q \& 2^{(p-1)/q} \equiv 1 \pmod p) = \frac{1}{q(q-1)}$. Putting everything together we get

$$\begin{aligned}\Pr(2 \text{ is a primitive root mod } p) &= \prod_{q \text{ prime}} \left(1 - \Pr(p \equiv 1 \pmod q \& 2^{(p-1)/q} \equiv 1 \pmod p)\right) \\ &= \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right).\end{aligned}$$

What about 2 or 3 a quadratic residue? The heuristic above suggests that

$$\Pr(2\&3 \text{ are primitive roots}) = \prod_{q \text{ prime}} \left(1 - \Pr(p \equiv 1 \pmod q \& (2^{(p-1)/q} \equiv 1 \pmod p \text{ OR } 3^{(p-1)/q} \equiv 1 \pmod p))\right).$$

Unpacking, $p \equiv 1 \pmod q$ occurs with probability $\frac{1}{q-1}$. We are then asking whether $2^{(p-1)/q}$ or $3^{(p-1)/q}$ is the root 1 of $X^q - 1 \pmod p$. This occurs with probability $\frac{2}{q} - \frac{1}{q^2}$. Putting everything together we get

$$\Pr(2\&3 \text{ are primitive roots}) = \prod_q \left(1 - \frac{1}{q-1}\left(\frac{2}{q} - \frac{1}{q^2}\right)\right) \approx 0.1476.$$

Finally,

$$\Pr(2 \text{ OR } 3 \text{ is a primitive roots}) = \Pr(2) + \Pr(3) - \Pr(2\&3) \approx 0.6005.$$

□

Lecture 15
2022-09-26

3.9 Quadratic residues modulo p

Fermat studied the question of when a prime can be written as $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$, etc.

Let $p \equiv 3 \pmod 4$. If $p = x^2 + y^2$ we already saw, as an application to Fermat's little theorem, that $p \mid x, y$ which would imply that $p^2 \mid x^2 + y^2 = p$, a contradiction.

Suppose we wanted to do the same type of argument for $p \mid x^2 + 2y^2$ or $p \mid x^2 + 3y^2$. We are asking whether $x, y \not\equiv 0 \pmod p$ can satisfy $x^2 + dy^2 \equiv 0 \pmod p$. In this case we'd have

$$-d \equiv (x/y)^2 \pmod p.$$

When $d = 1$, we settled this question easily. In general, it is the much harder classical question of when a residue $a \in \mathbb{Z}_p$ is equivalent to a perfect square $\pmod p$.

Definition 63. The **Legendre symbol** is a function $\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p \to \{-1, 0, 1\}$ defined as following

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod p \\ 1 & a \equiv x^2 \pmod p \text{ for some } x \in \mathbb{Z}_p^\times \\ -1 & \text{otherwise.} \end{cases}$$

Lemma 64. *Let $p > 2$ be a prime and let g be a primitive root modulo p.*

1. *An element $x = a^k \in \mathbb{Z}_p^\times$ is a quadratic residue iff k is even.*
2. *For any $a \in \mathbb{Z}_p$ we have $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.*
3. *The Legendre symbol is multiplicative, i.e., $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$.*

Proof. (1): Certainly, if k is even, then $x \equiv (g^{k/2})^2$ is quadratic. Reciprocally, if $x \equiv u^2 \pmod p$ and $u = g^t$ then $g^k \equiv g^{2t} \pmod p$. Then Lemma 53 implies that $p - 1 = \operatorname{ord}(g) \mid k - 2t$. Since p is odd, this implies that k must be even.

(2): If $a \equiv 0 \pmod p$ then the equality is clear. Note that $g^{(p-1)/2}$ is a root of $X^2 - 1 \pmod p$ so it is either 1 or -1. As $\operatorname{ord}(g) = p - 1$, it must be the latter so $g^{(p-1)/2} \equiv -1 \pmod p$. Suppose $a \equiv g^k \pmod p$. Then $a^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k \pmod p$ and this is 1 iff k is even. The equality then follows from (1).

(3): We simply check that $x^{(p-1)/2}$ is multiplicative. □

While Lemma 64 gives a convenient computation when $a = -1$:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

which is 1 iff $p \equiv 1 \pmod 4$ (or $p = 2$), in general the formula $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$ is computationally fast but rather opaque. Instead, we will transform this identity into a combinatorial computation, due to Gauss.

Lecture 16
2022-09-28

Today's lecture began with an aside on using CRT for solving equations.

Problem 65. Solve the equation $x^3 + x - 30 \equiv 0 \pmod{350}$.

Proof. This would be a nightmare to solve mod 350 directly. Instead, we'll use CRT as $350 = 2 \cdot 25 \cdot 7$. CRT says that knowing something mod 350 is equivalent to knowing that something separately mod 2, 25, and 7.

So let's solve $x^3 + x - 30 \equiv \pmod 2$, $\pmod{25}$, and $\pmod 7$.

Mod 2

Here $x^3 + x - 30 \equiv 0 \pmod 2$ is simply $x^3 + x \equiv 0 \pmod 2$, and $x \equiv 0, 1 \pmod 2$ both work.

Mod 7

We are solving $x^3 + x - 30 \equiv x^3 + x - 2 \equiv 0 \pmod 7$. We could do this by enumerating all the 7 residues mod 7. But we'll first factor $x^3 + x - 2 \equiv (x-1)(x^2 + x + 2) \equiv 0 \pmod 7$, for ease of testing the 7 cases. We see that the only possibilities that work are $x \equiv 1, 3 \pmod 7$.

CRT for 2 and 7

Since $2 \cdot 5 - 7 \cdot 2 = 15 - 14 = 1$ CRT is easy to apply:

$$x \equiv (0 \text{ or } 1) \cdot (-14) + (1 \text{ or } 3) \cdot 15 \equiv 1, 3, 8, 10 \pmod{14}.$$

Mod 25

We are solving $x^3 + x - 30 \equiv x^3 + x - 5 \pmod{25}$. We could simply enumerate every residue from 0 to 24. But if $x^3 + x - 5$ is a multiple of 25, it must also be a multiple of 5. Let's start with that: solve $x^3 + x - 5 \equiv x(x^2 + 1) \equiv 0 \pmod 5$, which holds only for $x \equiv 0, 2, 3 \pmod 5$.

Back to $x^3 + x - 5 \equiv 0 \pmod{25}$. Rather than checking every residue 0, 1, ..., 24, we only check those which are $\equiv 0, 2, 3 \pmod 5$:

$$0, 2, 3, 5, 7, 8, 10, 12, \underbrace{13, 15, 17, 18, 20, 22, 23}_{-12, -10, -8, -7, -5, -3, -2} \pmod{25}.$$

Checking each of these 15 possibilities (with, e.g., -3 instead of 22, for ease of arithmetic) we see that the solutions are $x \equiv 3, 5, 17 \pmod{25}$.

CRT for 14 and 25

Bézout is $14 \cdot 9 - 25 \cdot 5 = 126 - 125 = 1$ so CRT gives

$$x \equiv (1, 3, 8, \text{ or } 10) \cdot (-125) + (3, 5, \text{ or } 17) \cdot 126 \equiv 3, 17, 78, 80, 92, 155, 178, 192, 253, 255, 267, 330 \pmod{350}.$$

□

Going back to quadratic residues, recall that if we fixed a primitive root a, we were able to specify when a^k was a QR. Indeed, $a^k \equiv (a^\ell)^2$ means that $a^k \equiv a^{2\ell} \pmod p$ so $k \equiv 2\ell \pmod{p-1}$. This means that k has to be even, as 2ℓ and $p - 1$ are both even.

Aside: The idea that we might solve equations of the type $x^2 = y$ (or $x^{17} = y$) using exponentials $x = a^u$ rather than $x = \sqrt{y}$ (or $x = \sqrt[17]{y}$) is already present in calculus. Indeed, how to make sense of $\sqrt[17]{y}$ in a way that makes this expression have good properties? The easiest way is as follows:

$$\sqrt[17]{y} = y^{\frac{1}{17}} = (e^{\ln(y)})^{\frac{1}{17}} = e^{\frac{1}{17}\ln(y)}.$$

Now $\ln(y) = \int_1^y \frac{dt}{t}$ and $e^y = \ln^{-1}(y)$ so everything works as in calculus.

To solve equations of the form $x^2 \equiv y \pmod{p}$, when p is an odd prime, two ideas were essential:

1. Fermat's little theorem always holds. This means that if $x^2 \equiv y \pmod{p}$ has a solution, then **necessarily** $y^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. If this condition is not satisfied, then the equation can't possibly have a solution.

2. Suppose now that $y^{(p-1)/2} \equiv 1 \pmod{p}$, in which case Fermat's little theorem does NOT provide a contradiction. Why does this mean that $x^2 \equiv y \pmod{p}$ MUST have a solution, and, in fact, exactly two solutions? Here is where we choose some primitive root a and write $y = a^\ell$, $x = a^k$ and try to solve for k. As $y^{(p-1)/2} \equiv 1 \pmod{p}$, it means that $a^{\ell(p-1)/2} = (a^{(p-1)/2})^\ell \equiv (-1)^\ell \pmod{p}$ gives that ℓ must be even. Therefore $\ell = 2N$ so $x = \pm a^N$ are two solutions: $(\pm a^N)^2 = a^{2N} \equiv y \pmod{p}$.

In fact, we'll recall from the previous lecture that

$$\left(\frac{y}{p}\right) \equiv x^{(p-1)/2} \pmod{p}$$

specifies exactly whether y is a QR mod p.

3.10 Workshop on using primivite roots to solve some equations mod primes

Which of the following equations has a solution? How many solutions are there? How would you go about finding the solutions? All equations are modulo prime numbers. You can use wolframalpha for computations. For convenience, 2 is a primitive root mod 2027 and 2029, 3 is a primitive root mod 1999 and 2011, and 7 is a primitive root mod 997.

For the first three, the criterion above implies that it suffices to check whether $5^{(p-1)/2} \pmod{p}$, for which we used in class wolframalpha. We'll work on **solving** the equations next lecture.

1. $x^2 \equiv 5 \pmod{2011}$

   $5^{1005} \equiv 1 \pmod{2011}$ so there are exactly two solutions.

2. $x^2 \equiv 5 \pmod{2027}$

   $5^{1013} \equiv -1 \pmod{2027}$ so there are no solutions.

3. $x^2 \equiv 5 \pmod{2029}$

   $5^{1014} \equiv 1 \pmod{2029}$ so there are exactly two solutions.

For the cubes, we want to use, again, Fermat's little theorem: it is always true that $x^{p-1} \equiv 1 \pmod{p}$ if $p \nmid x$. So if $x^3 \equiv 5 \pmod{p}$ AND $p - 1 = 3N$ then it has to be the case that

$$x^{p-1} = x^{3N} \equiv 5^N \equiv 1 \pmod{p}.$$

This gives a criterion for when $x^3 \equiv 5 \pmod{p}$ does not have a solution.

4. $x^3 \equiv 5 \pmod{997}$

   Here $997 - 1 = 3 \cdot 332$ and $5^{332} \equiv 1 \pmod{997}$ so the equation MIGHT have solutions. Does it? Write everything in terms of the primitive root 7. Say $5 \equiv 7^k \pmod{997}$. Since $5^{332} \equiv 1$ it means that $7^{332k} \equiv 1 \pmod{997}$. But the only exponents of the primitive root which give 1 are the exponents $332k$ which are multiples of the order 996. So $332k = 996N$ so $k = 3N$ and we have our solution $x = 7^N$ as $x^3 = 7^{3N} = 7^k \equiv 5 \pmod{997}$. How many solutions there are is left for next lecture.

5. $x^3 \equiv 5 \pmod{1999}$

   Here $1999 - 1 = 3 \cdot 666$ and $5^{666} \equiv 808 \pmod{1999}$ so the equation has NO solutions.

6. $x^3 \equiv 5 \pmod{2027}$

   Here we seem to be in trouble, as we can't really use our idea with exponentiating $x^3 \equiv 5 \pmod{2027}$ to get Fermat's little theorem, as $2027 - 1 = 2026$ is not a multiple of 3. But, actually, in this case we've already done it before:

$$x = \text{“}\sqrt[3]{5}\text{”} \pmod{2027} = 5^{\text{“}3^{-1}\text{”}} \pmod{2027} \equiv 5^{3^{-1} \bmod 2026} \pmod{2027}.$$

   Since 3 and 2026 are coprime, 3 is invertible. **CAREFUL** here 3 has to be invertible, and its inverse computed, modulo $2026 = \varphi(2027)$ and not modulo 2027 itself. We get

$$x \equiv 5^{1351} \equiv 23 \pmod{2027}.$$

Lecture 17
2022-09-30

On the previous homework you had to show the following result:

Lemma 66. *Let p be a prime. Then the equation $x^n \equiv a \pmod{p}$ has either no solutions or exactly $(n, p-1)$ solutions modulo p.*

Remark 14. This is familiar even over the real numbers. How many **real** solutions does the equation $x^n = a$ have? It has 0 solutions if n is even and $a < 0$, it has 1 solution if n is odd or $a = 0$, and 2 solutions if n is even and $a > 0$.

Proof. Suppose $x^n \equiv a \pmod{p}$ has at least one solution, call it x_1. If x_2 is any other solution, then $x_1^n \equiv a \equiv x_2^n \pmod{p}$ so $(x_2/x_1)^n \equiv 1 \pmod{p}$. We get a bijection

$$\{\text{Roots of } x^n \equiv a \pmod{p}\} \leftrightarrow \{\text{Roots of } x^n \equiv 1 \pmod{p}\}$$

sending x_2 on the left to x_2/x_1. This is a bijection because any u on the right gives a root $x_2 = x_1 u$ on the left.

If $x^n \equiv a \pmod{p}$ has one solution, it must have precisely the same number of solutions as $x^n \equiv 1 \pmod{p}$. Now the roots of $x^n - 1$ in $\mathbb{Z}_p$ are all nonzero, so the are the roots of $x^n - 1$ which are in common with the set of roots $\{1, 2, \ldots, p-1\}$ of $x^{p-1} - 1 \bmod p$. But counting common roots of $x^n - 1$ and $x^{p-1} - 1$ can be done using the gcd, this being the number of roots of

$$(x^n - 1, x^{p-1} - 1) = x^{(n,p-1)} - 1,$$

which has precisely $(n, p-1)$ roots, by Lemma 59. □

Let's continue our previous examples and answer the question of what the solutions to these equations actually are? We are left with solving the following equations, for which we know solutions exist. One challenge is that, for practical purposes, we **cannot** use the exponent of the primitive root, as this discrete logarithm is not computationally feasible. Instead, we'll have to come up with indirect ways of gleaning information about this discrete logarithm.

1 $x^2 \equiv 5 \pmod{2011}$

   Primitive root 3. We write $x \equiv 3^k$ and $5 \equiv 3^\ell \pmod{2011}$. We are solving

$$3^{2k} \equiv 3^\ell \pmod{2011} \qquad \text{equivalently} \qquad 2k \equiv \ell \pmod{2010}.$$

   Let's solve the latter equation by pretending that we know what ℓ is. Well, $2010 = 2 \cdot 1005$ so we'll use CRT. We are solving

$$\begin{cases} 2k \equiv \ell \pmod{2} \\ 2k \equiv \ell \pmod{1005}. \end{cases}$$

We already know that a solution exists, so ℓ is even, in which case the first equation is automatically satisfied, giving $k \equiv 0, 1 \pmod 2$. We are now looking only at the second $2k \equiv \ell \pmod{1005}$. Crucially, we can invert 2! So $k \equiv 2^{-1}\ell \equiv 503\ell \pmod{1005}$. CRT then tells us that $k \equiv 503\ell, 503\ell + 1005 \pmod{2010}$. Therefore

$$x = a^k \equiv 3^{503\ell \text{ or } 503\ell+1005} \equiv (3^\ell)^{503} \text{ or } (3^\ell)^{503} \cdot 3^{1005} \equiv 5^{503} \text{ or } 5^{503} \cdot 3^{1005} \equiv \pm 5^{503} \equiv 540 \pmod{2011},$$

recalling here that $3^{1005} \equiv -1 \pmod{2011}$.

3 $x^2 \equiv 5 \pmod{2029}$

Primitive root 2. Again we solve $2k \equiv \ell \pmod{2028}$ and again we use CRT to solve

$$\begin{cases} 2k \equiv \ell \pmod 4 \\ 2k \equiv \ell \pmod{507}. \end{cases}$$

Let's ignore the first equation. Again we can solve the latter equation as $k \equiv 2^{-1}\ell \pmod{507} \equiv 254\ell \pmod{507}$. So we get that $k \equiv 254\ell + 507N \pmod{2028}$ for some $N = 0, 1, 2, 3$. These are not that many choices, so we could test them all:

$$x \equiv 2^k \equiv 2^{254\ell+507N} \equiv (2^\ell)^{254} \cdot (2^{507})^N \equiv 5^{254} \cdot 992^N \equiv 331 \cdot 992^N \pmod{2029}.$$

Checking each $N = 0, 1, 2, 3$ we see that the two solutions are $x \equiv \pm 346 \pmod{2029}$.

4 $x^3 \equiv 5 \pmod{997}$

Primitive root 7. We are solving $3k \equiv \ell \pmod{996}$ and, factoring into coprime to 3 and power of 3, CRT gives the equivalent system of equations

$$\begin{cases} 3k \equiv \ell \pmod 3 \\ 3k \equiv \ell \pmod{332}. \end{cases}$$

Forget about the first equation. The second one can be solved as

$$k \equiv 3^{-1}\ell \equiv 111\ell \pmod{332},$$

so $k \equiv 111\ell + 332N$ where $N = 0, 1, 2$. As before, we compute

$$x \equiv 7^{111\ell+332N} \equiv (7^\ell)^{111} \cdot (7^{332})^N \equiv 5^{111} \cdot 304^N \equiv 359 \cdot 304^N \pmod{997}.$$

Each of these three will be a solution: $x = 110, 348, 539 \pmod{997}$.

6 $x^3 \equiv 5 \pmod{2027}$

Primitive root 2. Again, we are solving $3k \equiv \ell \pmod{2026}$. But, since $3 \nmid 2026$, this has a single solution, which we already determined.

Lecture 18
2022-10-03

A more revealing example, which appears algorithmically in **Rabin's cryptosystem**, is the following:

Problem 67. The prime $p = 1601$ has 7 as a primitive root. Solve the equation $x^2 \equiv 5 \pmod{1601}$.

Proof. Let's try to do this as before: writing $x \equiv 7^k$ and $5 \equiv 7^\ell \pmod{1601}$ gives the equation $2k \equiv \ell \pmod{1600}$. Let's apply CRT again, but separating the powers of 2. Since $1600 = 2^6 \cdot 25$ we get

$$\begin{cases} 2k \equiv \ell \pmod{64} \\ 2k \equiv \ell \pmod{25}. \end{cases}$$

We could try doing the same thing as before, ignoring the first equation, and inverting 2 in the second one: $k \equiv 2^{-1}\ell \equiv 13\ell \pmod{25}$ so $k \equiv 13\ell + 25N \pmod{1600}$ for some $N = 0, 1, \ldots, 63$. We'd get

$$x \equiv 7^{13\ell+25N} \equiv (7^\ell)^{13} \cdot (7^{25})^N \pmod{1601},$$

and we'd have to go through the list of possible N-s and check which one gives $x^2 \equiv 5 \pmod{1601}$.

The challenge is that now the list of N-s to check is quite large. **Is there a fast way of going through this list, that doesn't make us check 64 different values?** In fact there is, and we'll be able to get by with checking only 6 (namely the exponent $64 = 2^6$) different values!

Let's look back at the possible values of x:

$$x \equiv 5^{13} \cdot (7^{25})^N \pmod{1601}.$$

To test whether this works, we'd have to check if

$$5 \equiv x^2 \equiv 5^{26} \cdot (7^{50})^N \pmod{1601}.$$

The idea is to use the general fact that $7^{800} \equiv -1 \pmod{p}$ (a primitive root to the $(p-1)/2$ in general). Raise to the 16th power! We'd need

$$5^{16} \equiv 5^{26\cdot 16} \cdot (7^{800})^N \equiv 5^{26\cdot 16} \cdot (-1)^N \pmod{1601}.$$

So $(-1)^N = 1$ so N **is even**. So we're only looking at $N = 2N_1$ with $N_1 = 0, 1, \ldots, 31$. Excellent, only half of the original list.

Now we're asking whether

$$x \equiv 5^{13} \cdot (7^{25})^{2N_1} \equiv 5^{13} \cdot (7^{50})^{N_1} \pmod{1601}$$

works, so we require

$$5 \equiv x^2 \equiv 5^{26} \cdot (7^{100})^{N_1} \pmod{1601}$$

and we can play the same game. To get to $7^{800} \equiv -1$ we only need to raise to the 8th power now.

$$5^8 \equiv 5^{26\cdot 8} \cdot (-1)^{N_1} \pmod{1601},$$

so $(-1)^{N_1} = -1$ so N_1 is odd. This means that $N_1 = 2N_2 + 1$ where $N_2 = 0, 1, \ldots, 15$. Excellent, we halved the list again! You can see where this is going.

We are checking if

$$x \equiv 5^{13} \cdot (7^{50})^{2N_2+1} \equiv 5^{13} \cdot 7^{50} \cdot (7^{100})^{N_2} \pmod{1601}$$

works, so we require

$$5 \equiv x^2 \equiv 5^{26} \cdot 7^{100} \cdot (7^{200})^{N_2} \pmod{1601}.$$

To get to $7^{800} \equiv -1$ we only need to raise to the 4th power now.

$$5^4 \equiv 5^{26\cdot 4} \cdot 7^{400} \cdot (-1)^{N_2} \pmod{1601},$$

so $(-1)^{N_2} = 1$ so $N_2 = 2N_3$ is even, with $N_3 = 0, 1, \ldots, 7$.

We keep going

$$x \equiv 5^{13} \cdot 7^{50} \cdot (7^{100})^{2N_3} \equiv 5^{13} \cdot 7^{50} \cdot (7^{200})^{N_3} \pmod{1601}.$$

The check requires

$$5 \equiv x^2 \equiv 5^{26} \cdot 7^{100} \cdot (7^{400})^{N_3} \pmod{1601}$$

we square to get

$$5^2 \equiv 5^{26\cdot 2} \cdot 7^{200} \cdot (-1)^{N_3} \pmod{1601}$$

giving $(-1)^{N_3} = 1$ so $N_3 = 2N_4$ is even, with $N_4 = 0, 1, 2, 3$.

Next:

$$x \equiv 5^{13} \cdot 7^{50} \cdot (7^{400})^{N_4} \pmod{1601}$$

giving the check:

$$5 \equiv x^2 \equiv 5^{26} \cdot 7^{100} \cdot (-1)^{N_4} \pmod{1601}$$

so $(-1)^{N_4} = 1$ so $N_4 = 0$ or 2. Finally, we get the two solutions

$$x \equiv 5^{13} \cdot 7^{50} \cdot (7^{400})^{0 \text{ or } 2} \equiv \pm 390 \pmod{1601}.$$

□

3.11 The Legendre symbol

We recalled the proof of Fermat's little theorem, which involved the permutation of $\mathbb{Z}_p^\times$ given by $a\mathbb{Z}_p^\times$. To compute the value of $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ using the same idea, we seek a subset $\mathcal{P} \subset \mathbb{Z}_p^\times$, with $\frac{p-1}{2}$ elements, and understand the set $a\mathcal{P}$. Many, though not all, such subsets will do, but in practice one chooses something very specific:

Theorem 68 (Gauss' Lemma)**.** *Let $p > 2$ be a prime and $\mathcal{P} = \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{|-\mathcal{P} \cap a\mathcal{P}|}.$$

Theorem 68 is typically used to compute $\left(\frac{2}{p}\right)$, which cannot be computed using quadratic reciprocity.

Corollary 69. *If $p > 2$ is a prime then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. In other words, $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$.*

Proof. It is the second statement, which is equivalent to the first one, that we'll deduce by applying Theorem 68. We need to compute the cardinality of

$$-\mathcal{P} \cap 2\mathcal{P} = \underbrace{\{\frac{p+1}{2}, \ldots, p-1\}}_{-\mathcal{P}} \cap \underbrace{\{2, 4, \ldots, p-1\}}_{2\mathcal{P}}.$$

I'll write here the case $p \equiv 3 \pmod{8}$, so $p = 8N + 3$. Then $-\mathcal{P} = \{4N + 2, \ldots, 8N + 2\}$, while $2\mathcal{P} = \{2, 4, \ldots, 8N + 2\}$. This means that $2\mathcal{P} \setminus (-\mathcal{P}) = \{2, 4, \ldots, 4N\}$ has $2N$ elements, so the intersection has $2N + 1$ elements, which gives $\left(\frac{2}{p}\right) = (-1)^{2N+1} = -1$.

The other cases will be left as homework.

□

Lecture 19
2022-10-05

Proof of Gauss' Lemma: What on earth is going on here?

Let's start unpacking the participants in this statement. We begin with $\mathcal{P}$:

$$-\mathcal{P} = \{-\overline{1}, -\overline{2}, \ldots, -\overline{\frac{p-1}{2}}\} = \{\overline{\frac{p+1}{2}}, \ldots, \overline{p-2}, \overline{p-1}\},$$

in other words, $\mathbb{Z}_p^\times = \mathcal{P} \sqcup -\mathcal{P}$.

But **why** would we care at all about $\mathcal{P}$? Recall that in proving Theorem 45 we used the fact that $a\mathbb{Z}_p^\times = \{ax \mid x \in \mathbb{Z}_p^\times\}$ produces a permutation of $\mathbb{Z}_p^\times$. Since permutation doesn't change the product of the elements we concluded that the a^{p-1} extra factors in the permuted $a\mathbb{Z}_p^\times$ must equal 1 (mod p).

From Lemma 64 we know that $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$. If we wanted to mimic the above idea, but to end up with only $a^{(p-1)/2}$, we had better replace $\mathbb{Z}_p^\times$ with a subset of cardinality $\frac{p-1}{2}$. That's where $\mathcal{P}$ comes in. In some sense, the choice of $\mathcal{P}$ matters for convenience, rather than for conceptual reasons.

Let's find out $a^{(p-1)/2}$. By $\prod(\mathcal{S})$ for a subset $\mathcal{S} \subset \mathbb{Z}_p$ we mean the product of all the elements of $\mathcal{S}$. Then

$$\begin{aligned}\prod(a\mathcal{P}) &= \prod_{x\in\mathcal{P}} ax \\ &= a^{(p-1)/2} \prod(\mathcal{P}).\end{aligned}$$

In the case of Euler's theorem, the final step came from $a\mathbb{Z}_p^\times = \mathbb{Z}_p^\times$. That will not be the case for $a\mathcal{P}$. However, whatever $a\mathcal{P}$ is in relation to $\mathcal{P}$, what we do know is that $a\mathcal{P} \subset a\mathbb{Z}_p^\times = \mathbb{Z}_p^\times$. This, in turn, is $\mathcal{P} \sqcup -\mathcal{P}$ so we conclude that

$$a\mathcal{P} \subset \mathcal{P} \sqcup -\mathcal{P}.$$

This means we can find some elements $x_1, \ldots, x_a, y_1, \ldots, y_b \in \mathcal{P}$ (with $a + b = \frac{p-1}{2}$) such that

$$a\mathcal{P} = \underbrace{\{x_1, \ldots, x_a\}}_{\subset\mathcal{P}} \sqcup \underbrace{\{-y_1, \ldots, -y_b\}}_{\subset -\mathcal{P}}.$$

It seems like we lost control of the "permutation" part from $a\mathbb{Z}_p^\times = \mathbb{Z}_p^\times$. However, we can get something very close using the following observation: $x_i \neq y_j$ for all i, j.

Setting aside why this is true, we conclude that $\{x_1, \ldots, x_a, y_1, \ldots, y_b\}$ form a permutation of $\mathcal{P}$ and so we can still use the idea of the product:

$$\begin{aligned}\prod(a\mathcal{P}) &= \prod x_i \prod(-y_j) \\ &= (-1)^b \prod x_i \prod y_j \\ &= (-1)^b \prod(\mathcal{P}),\end{aligned}$$

the desired result following from the fact that, by definition, $b = |-\mathcal{P} \cap a\mathcal{P}|$.

So why is it the case that $x_i \neq y_j$? What would happen if $x_i = y_j$? The LHS is of the form au and the RHS of the form $-av$ for some $u, v \in \mathcal{P}$, by definition. This would mean that $u = -v$ for $u, v \in \mathcal{P}$, but this contradicts the fact that $\mathcal{P} \sqcup -\mathcal{P} = \mathbb{Z}_p^\times$ is a **disjoint** union. □

3.12 Quadratic Reciprocity

One of the biggest theorems of the 19th century is the following:

Theorem 70 (Quadratic Reciprocity)**.** *Suppose p and q are odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Remark 15. If either p or q is $\equiv 1 \pmod 4$ then the exponent is even so we get

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \qquad\qquad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

If $p, q \equiv 3 \pmod 4$ then the exponent is odd so we get

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \qquad\qquad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

This was how quadratic reciprocity was known to Gauss, before the introduction of the Legendre symbol.

We won't be proving this theorem because, while it has hundreds of proofs, most are difficult to place in their appropriate contexts without a lot of extra background, which makes them seem hard to really understand. Instead, we will concentrate on its uses.

3.12.1 Application 1

Fast computation of the Legendre symbol.

3.12.2 Application 2

Quadratic reciprocity is well-suited for answering the question for what primes p is a a QR?

Problem 71. What primes numbers appear as divisors of some element of the set $\{n^2 - 6 \mid n \in \mathbb{Z}\}$?

Proof. A prime p divides some $n^2 - 6$ iff $6 \equiv n^2 \pmod p$ iff 6 is a quadratic residue mod p. Since $2, 3 \mid 0^2 - 6$, we may assume $p > 3$. Then we seek $p > 3$ prime such that $\left(\frac{6}{p}\right) = 1$. Proof continues next lecture.

Lecture 20
2022-10-07

Since $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$, we compute each factor separately. We already know that $\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod 8$. What about $\left(\frac{p}{3}\right)$? By Quadratic Reciprocity, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. Here $(-1)^{(p-1)/2} = 1$ iff $p \equiv 1 \pmod 4$ and $\left(\frac{p}{3}\right) = \left(\frac{p \bmod 3}{3}\right) = 1$ iff $p \equiv 1 \pmod 3$. We make a table of possible values of $\left(\frac{3}{p}\right)$, using CRT to fill it up:

	$\left(\frac{p}{3}\right) = 1,\ p \equiv 1 \pmod 3$	$\left(\frac{p}{3}\right) = -1,\ p \equiv -1 \pmod 3$
$(-1)^{(p-1)/2} = 1,\ p \equiv 1 \pmod 4$	$\left(\frac{3}{p}\right) = 1,\ p \equiv 1 \pmod{12}$	$\left(\frac{3}{p}\right) = -1,\ p \equiv 5 \pmod{12}$
$(-1)^{(p-1)/2} = -1,\ p \equiv -1 \pmod 4$	$\left(\frac{3}{p}\right) = -1,\ p \equiv -5 \pmod{12}$	$\left(\frac{3}{p}\right) = 1,\ p \equiv -1 \pmod{12}$

which gives $\left(\frac{3}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod{12}$.

We do the same to compute $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$, taking care with CRT (which a priori requires coprime moduli):

	$\left(\frac{3}{p}\right) = 1,\ p \equiv \pm 1 \pmod{12}$	$\left(\frac{3}{p}\right) = -1,\ p \equiv \pm 5 \pmod{12}$
$\left(\frac{2}{p}\right) = 1,\ p \equiv \pm 1 \pmod 8$	$\left(\frac{6}{p}\right) = 1,\ p \equiv \pm 1 \pmod{24}$	$\left(\frac{6}{p}\right) = -1,\ p \equiv \pm 7 \pmod{24}$
$\left(\frac{2}{p}\right) = -1,\ p \equiv \pm 3 \pmod 8$	$\left(\frac{6}{p}\right) = -1,\ p \equiv \pm 11 \pmod{24}$	$\left(\frac{6}{p}\right) = 1,\ p \equiv \pm 5 \pmod{24}$

For instance, what is $p \pmod{24}$ if $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 5 \pmod{12}$? The latter condition gives $p \equiv \pm 5, \pm 5 + 12 \pmod{24}$ and of these only $p \equiv 7, 17 \pmod{24}$ satisfy the former. The other three cases are similar.

We conclude that $p \mid n^2 - 6$ for some n if either $p = 2, 3$ or $p \equiv \pm 1, \pm 5 \pmod{24}$. □

3.13 Application 3

One final application is to show the infinitude of certain classes of primes.

Problem 72. Show that there are infinitely many primes:

1. With no conditions.
2. Which are $\equiv 1 \pmod 4$.
3. Which are $\equiv 3 \pmod 4$.
4. Which are $\equiv 1 \pmod 3$.
5. Which are $\equiv 2 \pmod 3$.

Proof. (1) Let p be any prime divisor of $n! + 1$. This means $n! \equiv -1 \pmod p$ so $p > n$, or else $n! \equiv 0 \pmod p$. This means that there exists a prime number $> n$, for any n, and therefore there exist infinitely many prime numbers.

(2) Let p be any prime divisor of $n!^2 + 1$. Again $p > n$ as above. Since $n!^2 \equiv -1 \pmod p$ we see that $\left(\frac{-1}{p}\right) = 1$ so $p \equiv 1 \pmod 4$.

(3) Factor $4n! - 1 = \prod p_i^{k_i}$ into primes. Each prime divisor, as above, will have to be $> n$. Moreover, if all $p_i \equiv 1 \pmod 4$ then $4n! - 1 \equiv \prod 1^{k_i} \equiv 1 \pmod 4$, which is clearly not true. Therefore at least one of these primes $p_i > n$ will have to be $\equiv 3 \pmod 4$. But then for every n there is a prime $\equiv 3 \pmod 4$ larger than n, and therefore infinitely many.

(4) Look at any prime divisor of $9n!^2 + 3$, other than 3.

(5) Some prime divisor of $3n! - 1$ will be $\equiv 2 \pmod 3$. □

Lecture 21
2022-10-10

---

4 Primes and valuations

One of the most momentous insights in number theory in the last century is that one can do calculus not only with real and complex numbers, but also with "p-adic" numbers, which are versions of the reals combined with prime factorizations.

What are some familiar Taylor expansions?

$$\begin{aligned}
\frac{1}{1-x} &= \sum x^n \\
e^x &= \sum \frac{x^n}{n!} \\
\sin x &= \sum (-1)^n \frac{x^{2n+1}}{(2n+1)!} \\
\cos x &= \sum (-1)^n \frac{x^{2n}}{(2n)!} \\
\arctan x &= \int \frac{dx}{x^2+1} \\
&= \sum (-1)^n \frac{x^{2n+1}}{2n+1} \\
\ln(1+x) &= \int \frac{dx}{1+x} \\
&= \sum (-1)^n \frac{x^n}{n}
\end{aligned}$$

the last two giving the useful formulas

$$\sum \frac{(-1)^n}{n} = \ln(2)$$
$$\sum \frac{(-1)^n}{2n+1} = \frac{\pi}{4}.$$

We also recall the binomial formula

$$(1+x)^N = \sum_{n=0}^{N} \binom{N}{n} x^n,$$

where

$$\binom{N}{n} = \frac{N!}{n!(N-n)!} = \frac{N(N-1)\cdots(N-(n-1))}{n!},$$

the latter formula having the advantage of being a polynomial of degree n in the variable N. As $\binom{N}{n} = 0$ whenever $n > N$, we can rewrite the binomial formula as a Taylor series

$$(1+x)^N = \sum_{n=0}^{\infty} \binom{N}{n} x^n.$$

This generalizes to all real exponents α, the Taylor expansion being

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n.$$

For instance,

$$\sqrt{1-x} = (1-x)^{1/2} = \sum_{n=0}^{\infty} \binom{1/2}{n} x^n.$$

Computing out the first few coefficients

$$\binom{1/2}{0} = 1$$
$$\binom{1/2}{1} = \frac{1}{2}$$
$$\binom{1/2}{2} = \frac{\frac{1}{2}(\frac{1}{2}-1)}{2!} = -\frac{1}{8}$$
$$\binom{1/2}{3} = \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)}{3!} = \frac{1}{16},$$

we get

$$\sqrt{1-x} = 1 - \frac{1}{2}x - \frac{1}{8}x^2 - \frac{1}{16}x^3 \cdots .$$

Note that if α is rational, so is $\binom{\alpha}{n}$ for all $n \geq 0$.

The goal of this chapter is to understand the prime factorizations of such Taylor coefficients.

4.1 p-valuations

Definition 73. Suppose p is a prime number and N is an integer. Then $v_p(N)$ is defined to be the exponent of p when we factor N into primes. Alternatively, $v_p(N)$ is the largest power of p which divides N.

We'll be able to compute the following:

1. $v_p(n!)$, which will lead to counting prime numbers.
2. $v_p(\binom{m}{n})$
3. $v_p(a^n - b^n)$, which we'll use to study primitive roots modulo prime powers.

Lemma 74. *If a, b are integers and p is a prime, then $v_p(ab) = v_p(a) + v_p(b)$. Moreover, $v_p(1) = 0$ and $v_p(0) = \infty$.*

Remark 16. The above lemma, whose proof I did in class, tells us that we can think of v_p as a kind of logarithm which ignores all primes in the prime factorization other than p.

We can now make sense of p-valuations even for rational numbers, if we want the above "log transforms products into sums" property to be true. Indeed,

$$v_p(a) = v_p(\frac{a}{b} \cdot b) = v_p(\frac{a}{b}) + v_p(b)$$

so $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$, computing the power of p in the factorization of $\frac{a}{b}$, with a negative sign if the power of p appears in the denominator.

4.2 Factorials

Theorem 75. *Let p be a prime number and $n \geq 0$ an integer.*

1. $v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$.
2. *Let $s_p(n)$ be the sum of the digits of n when written in base p. Then*

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}.$$

I worked out some examples in class, and noted that already the first part implies that

$$v_p(n!) < \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \frac{n}{p-1}.$$

As an application we got that $2^n \nmid n!$, a classical problem.

Proof. (1): This is a beautiful application of the idea underlying Fubini's theorem from multivariable calculus in the context of a double sum. It all comes down to the previous observation that $v_p(k)$ is the largest exponent of p which divides k, in other words

$$v_p(k) = \sum_{i \geq 1, p^i | k} 1.$$

We get that

$$\begin{aligned} v_p(n!) &= v_p(\prod_{k=1}^{n} k) \\ &= \sum_{k=1}^{n} v_p(k) \\ &= \sum_{k=1}^{n} \sum_{i \geq 1, p^i | k} 1 \\ &= \sum_{i=1}^{\infty} \sum_{k=1, p^i | k}^{n} 1. \end{aligned}$$

This last interior sum is easy to figure out. How many of the numbers of 1 to n are multiples of p^i? Exactly $\left\lfloor \frac{n}{p^i} \right\rfloor$: they are $1 \cdot p^i$, $2 \cdot p^i$, ..., $\left\lfloor \frac{n}{p^i} \right\rfloor \cdot p^i$. We get

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

as desired.

Lecture 22
2022-10-12

---

(2): Since we are dealing with integers written in base p, let's write $n = n_d \dots n_{0(p)}$. Then

$$\begin{aligned} v_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \\ &= \left\lfloor \frac{n_d \dots n_{0(p)}}{10_{(p)}} \right\rfloor + \left\lfloor \frac{n_d \dots n_{0(p)}}{100_{(p)}} \right\rfloor + \cdots \\ &= \lfloor n_d \dots n_1 . n_{0(p)} \rfloor + \lfloor n_d \dots n_2 . n_1 n_{0(p)} \rfloor + \cdots + \left\lfloor n_d . n_{d-1} \dots n_{0(p)} \right\rfloor \\ &= n_d \dots n_{1(p)} + n_d \dots n_{2(p)} + \cdots + n_d. \end{aligned}$$

Why is this equal to $\frac{n - s_p(n)}{p-1}$? Let's reverse engineer:

$$\begin{aligned} \frac{n - s_p(n)}{p-1} &= \frac{n_d \dots n_{0(p)} - (n_d + \cdots + n_0)}{p-1} \\ &= \frac{n_d p^d - n_d + n_{d-1} p^{d-1} - n_{d-1} + \cdots + n_1 p - n_1}{p-1} \\ &= n_d \frac{p^d - 1}{p-1} + n_{d-1} \frac{p^{d-1} - 1}{p-1} + \cdots + n_1 \frac{p-1}{p-1}. \end{aligned}$$

These two expressions are the same because of the geometric series formula.

□

At the start of the lecture, I added the following example, similar to the first part of the theorem:

Problem 76. What is $v_p\left(\prod_{k=1}^{n} k^k\right)$? (This quantity appears in arithmetic a few times.)

Proof. Using the idea that $v_p(k) = \sum_{i \geq 1, p^i | k} 1$ we have

$$\begin{aligned} v_p\left(\prod_{k=1}^{n} k^k\right) &= \sum_{k=1}^{n} k v_p(k) \\ &= \sum_{k=1}^{n} \sum_{i \geq 1, p^i | k} k \\ &= \sum_{i=1}^{\infty} \sum_{1 \leq k \leq n, p^i | k} k \\ &= \sum_{i=1}^{\infty} \left(p^i \cdot 1 + p^i \cdot 2 + \cdots + p^i \cdot \left\lfloor \frac{n}{p^i} \right\rfloor\right) \\ &= \sum_{i=1}^{\infty} \frac{1}{2} p^i \left\lfloor \frac{n}{p^i} \right\rfloor \left(\left\lfloor \frac{n}{p^i} \right\rfloor + 1\right). \end{aligned}$$

□

4.3 Binomial coefficients

Factorials are not the only kinds of combinatorial numbers that show up in Taylor expansions. We have the following beautiful result:

Theorem 77 (Kummer)**.** *Let p be a prime. Then $v_p\left(\binom{m}{n}\right)$ equals the number of carries one requires when performing the addition $n + (m - n) = m$ in base p.*

Lecture 23
2022-10-14

Whereas factorials are always divisible by high powers of p, we see that binomial coefficients have small exponents in their prime factorization. In fact, we have the following wonderful consequence:

Corollary 78. *Suppose we factor $\binom{m}{n} = p_1^{k_1} \cdots p_r^{k_r}$ into prime powers. Then each prime power is $p_i^{k_i} \leq m$.*

Proof. Say p^k is one of these prime factors. By Kummer's theorem, $k = v_p\left(\binom{m}{n}\right)$ equals the number of carries when adding $n + (m - n) = m$ in base p. If m has $d + 1$ digits in base p then, adding $n + (m - n)$ we can get at most d carries. But then $k = d$ and so $p^k = p^d \leq m$ as desired. □

Let's see an example of such binomial coefficient that appears naturally.

Problem 79. Compute the Taylor expansion of $\sqrt{1 + x}$ around 0.

Proof. We know that $\sqrt{1 + x} = \sum_{n=0}^{\infty} \binom{1/2}{n} x^n$ (what is the Taylor coefficient in general?) so we only need to evaluate the binomial coefficient.

$$\begin{aligned} \binom{1/2}{n} &= \frac{\frac{1}{2}\left(\frac{1}{2} - 1\right)\left(\frac{1}{2} - 2\right) \cdots \left(\frac{1}{2} - (n-1)\right)}{n!} \\ &= \frac{\frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right) \cdots \left(-\frac{2n-3}{2}\right)}{n!} \\ &= \frac{(-1)^{n-1} 1 \cdot 3 \cdots (2n-3)}{2^n n!}. \end{aligned}$$

There's a fancy notation for the numerator: $(2n-3)!! = 1 \cdot 3 \cdot 5 \cdots (2n-3)$, but it's only notation. The mathematical point, however, is that we can make this look like a binomial coefficient, namely by making the numerator look like a factorial. What's missing? The evens:

$$\begin{aligned}\binom{1/2}{n} &= \frac{(-1)^{n-1}(2n-2)!}{2^n n! 2 \cdot 4 \cdots (2n-2)} \\ &= \frac{(-1)^{n-1}(2n-2)!}{2^n n! (2 \cdot 1) \cdot (2 \cdot 2) \cdots (2 \cdot (n-1))} \\ &= \frac{(-1)^{n-1}(2n-2)!}{2^{2n-1} n! (n-1)!)}.\end{aligned}$$

This still doesn't look like a binomial coefficient:

$$\begin{aligned}\binom{1/2}{n} &= \frac{(-1)^{n-1}(2n-2)!(2n-1)(2n)}{2^{2n-1} n! (n-1)! (2n-1)(2n)} \\ &= \frac{(-1)^{n-1}(2n)!}{2^{2n} n!^2 (2n-1)} \\ &= \frac{(-1)^{n-1}}{2^{2n}(2n-1)} \binom{2n}{n}.\end{aligned}$$

□

Alright, so $\binom{2n}{n}$ appears naturally in Taylor series. Let's see what we can say by factorization.

Example 80. We have

$$\binom{1000}{500} = 2^6 \cdot 3^4 \cdot 5 \cdots 997.$$

Since each prime power is ≤ 1000 we get that

$$\binom{1000}{500} \leq 1000^{\pi(1000)}.$$

Let's see if we can find a lower bound. The coefficient $\binom{1000}{500}$ counts how many ways we can choose 500 elements among 1000 elements. What if we restrict attention to choosing these 500 elements as follows: the first element you choose from $\{1, 501\}$, the second from $\{2, 502\}$, ..., the 500th you choose from $\{500, 1000\}$. There is a total of 2^{500} ways to choose this way, so $2^{500} < \binom{1000}{500}$. We get

$$2^{500} < 1000^{\pi(1000)}$$

so

$$\pi(1000) > \frac{\ln(2^{500})}{\ln(1000)} = \frac{\ln(2)}{2} \cdot \frac{1000}{\ln(1000)}.$$

Lecture 24
2022-10-24

We saw in previous lectures that $v_p(n!) \approx \frac{n}{p-1}$, which grows linearly in n, but $v_p(\binom{m}{n})$ is the number of carries when adding $n + (m-n)$ in base p, which grows at most logarithmically in m. As a matter of fact, the p-valuation can be 0, which means that $\binom{m}{n} \not\equiv 0 \pmod{p}$. In fact, we can compute this residue.

Theorem 81 (Lucas)**.** *Suppose $m = m_d \ldots m_0{}_{(p)}$ and $n = n_d \ldots n_0{}_{(p)}$ are two numbers written in base p (the digits, even the leading ones, are allowed to be 0). Then*

$$\binom{m}{n} \equiv \binom{m_d}{n_d} \cdots \binom{m_1}{n_1} \binom{m_0}{n_0} \pmod{p}.$$

Proof. Let's first show that if $0 \le b \le a < p$ then $\binom{mp+a}{np+b} \equiv \binom{m}{n}\binom{a}{b} \pmod p$. Then Lucas' theorem will follow by induction.

We'll use the binomial expansion: the coefficient $\binom{mp+a}{np+b}$ is the coefficient of X^{np+b} in $(1+X)^{mp+a}$. From homework we know that $(u+v)^p \equiv u^p + v^p \pmod p$ so we get that

$$(1+X)^{mp+a} = ((1+X)^p)^m \cdot (1+X)^a \equiv (1+X^p)^m \cdot (1+X)^a \pmod p.$$

Now we use the binomial expansion on the RHS and get that $\binom{mp+a}{np+b}$ is the coefficient of X^{np+b} in

$$\sum_{i=0}^{m} \binom{m}{i} X^{pi} \sum_{j=0}^{a} \binom{a}{j} X^j \equiv \sum_{i=0}^{m}\sum_{j=0}^{a} \binom{m}{i}\binom{a}{j} X^{pi+j} \pmod p.$$

(In class I wrote this in a table form.)

Let's figure out which of the monomial terms give the desired X^{np+b}. We'd want $pi + j = np + b$. Now $0 \le j \le a < p$ so the only way $b - j$ is a multiple of p is if $b = j$, in which case $i = n$. Therefore, the term X^{np+b} shows up only once in the above sum, and its coefficient is $\binom{m}{n}\binom{a}{b}$, as desired. □

Example 82.

1. $\binom{47}{23} = \binom{142_{(5)}}{043_{(5)}} \equiv \binom{1}{0}\binom{4}{4}\binom{2}{3} \equiv 0 \pmod 5$, which makes sense as $23+24 = 43_{(5)} + 44_{(5)} = 142_{(5)}$ has 1 carry.
2. $\binom{49}{23} = \binom{144_{(5)}}{043_{(5)}} \equiv \binom{1}{0}\binom{4}{4}\binom{4}{3} \equiv 4 \pmod 5$.
3. Suppose we expand
$$(1+X)^{67} = 1 + \binom{67}{1}X + \binom{67}{2}X^2 + \cdots + X^{67}.$$
There are a total of 68 terms, all of them nonzero. How many terms survive when we reduce modulo 5? We get, by inspection,
$$(1+X)^{67} \equiv 1 + 2X + X^2 + 3X^5 + \cdots + X^{67}.$$
How many monomials are left? In other words, how many of the coefficients $\binom{67}{k} \not\equiv 0 \pmod 5$?
Lucas' Theorem tells us to write everything in base 5, so we write $k = abc_{(5)}$, allowing a, b, c to be 0. Then
$$\binom{67}{k} = \binom{232_{(5)}}{abc_{(5)}} \equiv \binom{2}{a}\binom{3}{b}\binom{2}{c} \pmod 5.$$
The only way this is not 0 is if each of the three factors $\binom{2}{a}$, $\binom{3}{b}$, and $\binom{2}{c}$ is nonzero mod 5, so we must have $a \le 2$, $b \le 3$, and $c \le 2$. In total 3 choices for a, 4 for b, and 3 for c, for a total of 36 choices, and therefore 36 monomials in $(1+X)^{67} \pmod 5$.

One final application of Lucas' theorem.

Example 83. Suppose p is a prime and n is a positive integer. What is

$$\sum_{p-1 \mid k} \binom{n}{k} \pmod p?$$

We begin with

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k,$$

and let's add over the values $x = 1, 2, \ldots, p-1$. Recall from a previous lecture that $\sum_{x=1}^{p-1} x^k \equiv 0 \pmod{p}$ if $p-1 \nmid k$, and $\equiv -1 \pmod{p}$ otherwise. This means that

$$\sum_{k=1}^{p-1}(1+x)^n = \sum_{x=1}^{p-1}\sum_{k=0}^{n}\binom{n}{k}x^k \equiv -\sum_{p-1|k}\binom{n}{k} \pmod{p}.$$

Here we can ignore $k \leq n$ as $\binom{n}{k} = 0$ whenever $k > n$.

On the LHS we have

$$2^n + 3^n + \cdots + p^n \equiv \sum_{x=1}^{p-1} x^n - 1 \pmod{p}$$

so

$$\sum_{p-1|k}\binom{n}{k} \equiv \begin{cases} 1 \pmod{p} & p-1 \nmid n \\ 2 \pmod{p} & p-1 \mid n \end{cases}.$$

Lecture 25
2022-10-26

4.4 Asymptotics of integer functions and The Prime Number Theorem

A huge achievement of 19th century number theory is an estimate of how many primes there are up to X. What do we mean by an asymptotic estimate of an integer function?

Suppose $C(n)$ is a function which counts objects "up to n". Some examples:

Number of	Exact count	Estimate
Positive integers $\leq n$	n	–
Perfect squares $\leq n$	$\lfloor\sqrt{n}\rfloor$	–
Integer solutions to $5x + 7y = 3$ with $\lvert x\rvert, \lvert y\rvert \leq n$	?	?
Fractions in the set $\{\frac{a}{b} \mid 1 \leq a, b \leq n\}$	?	?
Square-free positive integers $\leq n$	?	?
Monic polynomials mod p of degree n	?	?
Monic **irreducible** polynomials mod p of degree n	?	?
Primes $\leq n$	$\pi(n)$	?

Definition 84. An **asymptotic estimate** for an integer function $C(n)$ is a "nice" function $f(x)$, typically smooth, such that $C(n) \approx f(n)$ as $n \to \infty$. The asymptotic approximation is often controlled by finding a bound for the error $\lvert C(n) - f(n)\rvert$.

Theorem 85 (Prime Number Theorem)**.** *We have*

$$\pi(X) \approx \frac{X}{\ln X}.$$

A much better approximation is

$$\pi(X) \approx \int_2^X \frac{dt}{\ln t}.$$

We won't prove this result formally, mainly because any elementary proof would not keep the error term small enough. Instead, we'll sketch the logic of how one could get a handle on $\pi(X)$ and, in the process, see where the two mysterious functions in the theorem, particularly the second approximations, show up.

Our starting point is $n!$. We know that

$$n! = \prod_p p^{v_p(n!)}$$
$$\ln n! = \sum_p v_p(n!) \ln p.$$

We know that $v_p(n!) = \dfrac{n - s_p(n)}{p-1} \approx \dfrac{n}{p-1} \approx \dfrac{n}{p}$ so we get

$$\ln n! \approx \sum_p \frac{n}{p} \ln p$$
$$\sum_{k=1}^{n} \ln k \approx n \sum_{p \leq n} \frac{\ln p}{p}.$$

But $\displaystyle\sum_{k=1}^{n} \ln k \approx \int_1^n \ln t dt = n \ln n - n$ so we get

$$\ln n - 1 \approx \sum_{p \leq n} \frac{\ln p}{p}.$$

Proof continued next lecture.

Lecture 26
2022-10-28

Last lecture we were at the stage where

$$\sum_{p \leq n} \frac{\ln p}{p} \approx \ln n.$$

In order to approximate the number of primes up to n we could take all of these approximations and "solve" all these linear equations. But how to do this in practice? We can rewrite this approximation as

$$\sum_{k=2}^{n} \frac{\ln k}{k} \operatorname{IsPrime}(k) \approx \ln n,$$

where $\operatorname{IsPrime}(k) = 1$ if k is prime, and 0 otherwise.

Thinking about the function IsPrime we noted that $\operatorname{IsPrime}(k) = \pi(k) - \pi(k-1)$, which is nice, as it introduces $\pi(n)$ directly into the approximations. But we have no chance of obtaining something as calculusy as the Prime Number Theory unless we seek calculus. Graphing $\pi(x)$ as a real function, we noted that

$$\operatorname{IsPrime}(x) = d\pi(x)$$

is 1 precisely when x is an integer prime, and 0 otherwise. This, of course, is quite meaningless as $\pi(x)$ is not a differentiable function. But, if it were, we'd be able to rewrite our approximation as

$$\sum_{k=2}^{n} \frac{\ln(k)}{k} \operatorname{IsPrime}(k) = \int_2^n \frac{\ln x}{x} d\pi(x) \approx \ln n.$$

We will now think from an engineering point of view: instead of finding an approximation of $\pi(x) \approx f(x)$ directly, we first seek a **model** for $\pi(x)$. The model we'll use is the following: we will approximate $\pi(x)$ by a differentiable function $f(x)$ satisfying

$$\int_2^x \frac{\ln t}{t} df(t) = \ln x.$$

Then, because the above differential equation is approximately satisfied by π when x is an integer, we'll take the solution to this differential equation $f(x)$ to be an approximation to $\pi(x)$. Of course, what's lost in this model is **how good** an approximation $f(x)$ this differential equation produces. That is beyond the scope of this course.

Let's get back to the model, and solve the differential equation

$$\int_2^x \frac{\ln t}{t} df(t) = \ln x.$$

How would you solve it? Differentiating, we get

$$\begin{aligned} \frac{\ln x}{x} df(x) &= \frac{1}{x} \\ df(x) &= \frac{1}{\ln x}. \end{aligned}$$

By integrating, we get the approximation $\pi(x) \approx f(x) = \displaystyle\int_2^X \frac{dt}{\ln t}$.

This model is excellent for obtaining approximations for complicated expressions using primes.

Problem 86. Show that $\displaystyle\sum_{p \le n} p \approx \frac{n^2}{2 \ln n}$. (Contrast this with $\sum_{k=1}^n k \approx \frac{n^2}{2}$.)

Proof. We'll use the approximation $\pi(x)$ which satisfies the differential equation $d\pi(x) \approx \frac{1}{\ln x}$. Then

$$\begin{aligned} \sum_{p \le n} p &= \sum_{k=2}^n k \operatorname{IsPrime}(k) \\ &= \int_2^n x d\pi(x) \\ &\approx \int_2^n \frac{x}{\ln x} dx \\ &= \int_2^n \frac{2x}{\ln(x^2)} dx \\ &= \int_4^{n^2} \frac{dt}{\ln t} \\ &\approx \frac{n^2}{\ln(n^2)} \approx \frac{n^2}{2 \ln n}. \end{aligned}$$

□

Lecture 27
2022-10-31

4.5 Lifting the exponent

A marvelous result, originally appearing in an article by Mihai Manea, and now known as "lifting the exponent" is very useful in elementary number theory settings.

Theorem 87 (LTE)**.** *Suppose p is a prime number and $a, b \not\equiv 0 \pmod p$. If $a \equiv b \pmod p$ ($a \equiv b \pmod 4$ when $p = 2$) then*

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Example 88. Let's try to compute $v_3(23^{54} - 5^{54})$. Since $v_3(23 - 5) = 2 > 1$ we can apply LTE to get

$$v_3(23^{54} - 5^{54}) = v_3(23 - 5) + v_3(54) = 2 + 3 = 5.$$

Example 89. What is $v_2(3^n - 1)$? We can't apply LTE directly because $v_2(3 - 1) = 1$ instead of ≥ 2. In fact, when n is odd we see that $3^n - 1 \equiv (-1)^n - 1 \equiv 2 \pmod 4$ and so, while $3^n - 1$ is even, it is not a multiple of 4 so $v_2(3^n - 1) = 1$. But if n is even, we can use the previous idea. Write $n = 2m$

$$v_2(3^n - 1) = v_2(9^m - 1) = v_2(9 - 1) + v_2(m) = 3 + v_2(m) = 2 + v_2(n).$$

In particular,

$$v_2(3^{2^n} - 1) = n + 2.$$

Example 90. What is $v_7(11^n + 53^n - 2^{2n+1})$? We begin with

$$11^n + 51^n - 2^{2n+1} = 11^n - 4^n + 53^n - 4^n.$$

We can figure out the power of 7 in each of the two subtractions separately:

$$v_7(11^n - 4^n) = v_7(11 - 4) + v_7(n) = 1 + v_7(n)$$
$$v_7(53^n - 4^n) = v_7(53 - 4) + v_7(n) = 2 + v_7(n).$$

Let's say that $d = v_7(n)$. This means that 7^{d+1} is the exact power of 7 that divides $11^n - 4^n$ and 7^{d+2} is the exact power of 7 that divides $53^n - 4^n$. In any case, 7^{d+1} divides them both so it divides their sum. But 7^{d+2} can't divide the sum, because then it would have to divide $11^n - 4^n$. This means that the power of 7 in the sum is $d + 1$ so

$$v_7(11^n + 53^n - 2^{2n+1}) = 1 + v_7(n).$$

An amazing application of LTE is to describing $\mathbb{Z}_{p^n}^\times$ when p is a prime. We begin with the case $p = 2$.

Proposition 91. *If $n \geq 2$ then $\mathbb{Z}_{2^n}^\times = \{\pm 1, \pm 3, \ldots, \pm 3^{2^{n-2}-1}\}$.*

Proof. Both sides have 2^{n-2} elements so it's enough to check that the elements on the RHS are all distinct. Let's check that $\pm 3^i \not\equiv \pm 3^j \pmod{2^n}$ for $0 \leq i, j < 2^{n-2}$ unless they have the same sign and the same exponent.

We start by computing the multiplicative order of 3 (mod 2^n). Since $3^{2^{n-2}} \equiv 1 \pmod{2^n}$ (because $v_2(3^{2^{n-2}} - 1) = n$), the order has to be a divisor of 2^{n-2}. To check that it is exactly this, we'd have to check what $3^{2^{n-3}}$ is (mod 2^n). Can $3^{2^{n-3}} \equiv 1 \pmod{2^n}$? If so, it would mean that $v_2(3^{2^{n-3}} - 1) \geq n$, but we know this is $n - 1$. But $3^{2^{n-3}} \equiv 1 \pmod{2^{n-1}}$, so $3^{2^{n-3}} \equiv 1$ or $1 + 2^{n-1} \pmod{2^n}$? It's not 1 so it has to be the former.

We start with the case when they have the same sign. Then $3^{i-j} \equiv 1 \pmod{2^n}$ which implies that $2^{n-2} \mid i - j$, and this can only happen when $i = j$. What about the opposite sign case? We'd need $3^{i-j} \equiv -1 \pmod{2^n}$. It seems we are at a loss what to do. Taking cue from solving quadratics mod primes, we'll square this and derive some consequences first. We'd get $3^{2(i-j)} \equiv 1 \pmod{2^n}$ so we'd need $2^{n-2} \mid 2(i - j)$. If the exponents are distinct, this can only happen if $i - j = 2^{n-3}$. But then $3^{i-j} = 3^{2^{n-3}}$ and we already know that this is $1 + 2^{n-1} \not\equiv -1 \pmod{2^n}$. □

Remark 17. The same holds if we replace 3 with 5.

Proof of Theorem 87 by well-chosen example. Let's verify that

$$v_3(23^{54} - 5^{54}) = v_3(23 - 5) + v_3(54).$$

Since the answer involves $23 - 5 = 18$ let's use it in conjunction with the binomial formula

$$\begin{aligned} 23^{54} - 5^{54} &= (5+18)^{54} - 5^{54} \\ &= 5^{54} + \binom{54}{1}5^{53}\cdot 18 + \binom{54}{2}5^{52}\cdot 18^2 + \cdots + 18^{54} - 5^{54} \\ &= \binom{54}{1}5^{53}\cdot 18 + \binom{54}{2}5^{52}\cdot 18^2 + \cdots + 18^{54}. \end{aligned}$$

Now let's look at the valuations of the individual terms in the sum

$$23^{54} - 5^{54} = \underbrace{\binom{54}{1}5^{53}\cdot 18}_{v_3(54)+v_3(18)=5} + \underbrace{\binom{54}{2}5^{52}\cdot 18^2}_{v_3(\binom{54}{2})+v_3(18^2)=7} + \cdots + \underbrace{18^{54}}_{v_3(18^{54})=108}.$$

The thing to notice is that all terms, except for the first one, are multiples of 3^6. This means that the entire sum is a multiple of 3^5 but not of 3^6 so the valuation equals the valuation of only the first term, namely $v_3(54) + v_3(18) = 5$.

The general proof works identically, the first term giving the formula in LTE. □

Lecture 28
2022-11-02

While LTE was stated and proved only for integers, in fact it makes sense for algebraic integers, i.e., roots of monic polynomials with integer coefficients. This allows a marvelous application to the Fibonacci numbers.

Example 92. Recall that

$$F_n = \frac{\rho^n - \overline{\rho}^n}{\sqrt{5}}.$$

1. If $m \mid n$ then $F_m \mid F_n$.
2. If $p \mid F_d$ then $v_p(F_{dn}) = v_p(F_d) + v_p(n)$. In particular, the smallest index n such that F_n is a multiple of 25 is F_{25}.

I wrote out why if $n = md$ then $\frac{F_n}{F_m}$ involves Lucas numbers, and worked out the LTE computation for the second part.

4.6 Primitive roots modulo prime powers

One of the most beautiful applications of LTE is to show the existence of primitive roots mod prime powers.

Theorem 93. *If $p > 2$ is a prime, there exists a primitive root g modulo p^n, i.e., an element $g \in \mathbb{Z}_{p^n}^\times$ of order precisely $\varphi(p^n) = p^{n-1}(p-1)$. Equivalently,*

$$\mathbb{Z}_{p^n}^\times = \{1, g, g^2, \ldots, g^{\varphi(p^n)-1}\}.$$

Proof. Again, here's a proof by well-chosen example. Say we want to show the existence of a primitive root mod 7^n.

We begin with a primitive root modulo 7, and we can choose 3. (Check it.)

We'll show that $g = 3^7 \cdot 8 \in \mathbb{Z}_{7^n}^\times$ is a primitive root, for all exponents n. Here 3 is any primitive root mod $p = 7$, the exponent of 3 is $p = 7$, and $8 = p + 1$. We need to check that $3^7 \cdot 8$ has order exactly $\varphi(7^n) = 7^{n-1} \cdot 6$. How do we check this? We need

1. $(3^7 \cdot 8)^{7^{n-1}\cdot 6} \equiv 1 \pmod{7^n}$ (automatic by Euler).

2. $(3^7 \cdot 8)^{7^{n-2}\cdot 6} \not\equiv 1 \pmod{7^n}$.

3. $(3^7 \cdot 8)^{7^{n-1}\cdot 2} \not\equiv 1 \pmod{7^n}$.

4. $(3^7 \cdot 8)^{7^{n-1}\cdot 3} \not\equiv 1 \pmod{7^n}$.

For the last two, we note that if $\ell = 2, 3$ then

$$(3^7 \cdot 8)^{7^{n-1}\cdot \ell} \equiv 1 \pmod{7^n}$$

would also mean the same congruence (mod 7). But modulo 7, this is not true as the LHS is $\equiv 3^\ell \not\equiv 1$ (mod 7) as 3 has order 6, being a primitive root mod 7.

We only need to check the second congruence. But

$$\begin{aligned}(3^7 \cdot 8)^{7^{n-2}\cdot 6} &\equiv 3^{\varphi(7^n)} \cdot 8^{7^{n-2}\cdot 6} \pmod{7^n} \\ &\equiv 8^{7^{n-2}\cdot 6} \pmod{7^n}.\end{aligned}$$

Can this be $\equiv 1 \pmod{7^n}$? If so, then $7^n \mid 8^{7^{n-2}\cdot 6} - 1$ or $v_7(8^{7^{n-2}\cdot 6} - 1) \geq n$. But LTE gives that

$$v_7(8^{7^{n-2}\cdot 6} - 1) = v_7(8-1) + v_7(7^{n-2} \cdot 6) = n - 1.$$

□

We begin with a generalization of Wilson's theorem.

Example 94. Suppose $p > 2$ is a prime. What is

$$\prod_{1 \leq k < p^n, p \nmid k} k \pmod{p^n}?$$

The k varies in the set $\mathbb{Z}_{p^n}^\times$, which we know to be the same as $\{1, g, \ldots\}$ for a primitive root g modulo p^n. This means that

$$\begin{aligned}\prod_{1 \leq k < p^n, p \nmid k} k \pmod{p^n} &= \prod_{x \in \mathbb{Z}_{p^n}^\times} x \\ &= \prod_{k=0}^{\varphi(p^n)-1} g^k \\ &= g^{\sum_{k=0}^{\varphi(p^n)-1} k} = g^{\varphi(p^n)(\varphi(p^n)-1)/2}.\end{aligned}$$

Since $\varphi(p^n) = p^{n-1}(p-1)$ is even, we can rewrite this as

$$(g^{\varphi(p^n)/2})^{\varphi(p^n)-1}.$$

But, by Euler, anything to the power $\varphi(p^n)$ gives the answer 1, so this is simply

$$g^{-\varphi(p^n)/2}$$

What is this? Recall how we computed the Legendre symbol. This number is the root of $x^2 - 1 \pmod{p^n}$. This means $p^n \mid (x-1)(x+1)$ and, because $x+1$ and $x-1$ can't both be multiples of p (as $p > 2$) so either $x \equiv 1$ or $-1 \pmod{p^n}$. Can $g^{-\varphi(p^n)/2}$ be 1? No, because the order is precisely $\varphi(p^n)$, therefore the answer is -1. We end up with

$$\prod_{1 \leq k < p^n, p \nmid k} k \pmod{p^n} \equiv -1 \pmod{p^n}.$$

Lecture 29
2022-11-04

---

5 Continued Fractions

Let's begin with a classical question.

Problem 95. For what n is the sum of the first n integers a perfect square?

Suppose $1+2+\cdots+n=m^2$. This means $\frac{n(n+1)}{2}=m^2$ so $n^2+n=2m^2$. Trying to solve for n we see that

$$n=\frac{-1\pm\sqrt{1+8m^2}}{2}$$

so for this to be integer it had better be the case that the discriminant is a perfect square:

$$1+8m^2=x^2.$$

Writing $x=2m$ we get the famous Pell's equation:

$$x^2-2y^2=1.$$

For instance, $x=3$, $y=2$ is a solution, leading to $n=\frac{-1+x}{2}=1$. Another solution is $x=17$, $y=12$ giving $n=8$. Indeed, $1+2+\cdots+8=6^2$ is a perfect square.

How would we go about finding all solutions? We could try to divide by y

$$\left(\frac{x}{y}\right)^2-2=\frac{1}{y^2}\approx 0$$

so $\frac{x}{y}\approx\sqrt{2}$.

Of course not every rational approximation of $\sqrt{2}$ is good enough, we need one where the error is quadratic in the denominator. For instance,

$$\sqrt{2}=1.4142135\ldots\approx\frac{14142135}{10^7}$$

but $x=14142135$ and $y=10^7$ would give

$$x^2-2y^2=-17641775.$$

What we'd like, then, is to find some truly exceptional rational approximations to an irrational number, such as $\sqrt{2}$. That's where continued fractions come into play.

Definition 96. A continued fraction is an expression of the form

$$[a_0,a_1,\ldots]=a_0+\frac{1}{a_1+\frac{1}{a_2+\cdots}}.$$

Many issues arise from this notation, not least of which is that of convergence. Why does such a nested sequence of fractions ever converge?

Let's try the simples example:

Example 97. The continued fraction $[1,1,\ldots]$ converges to $\frac{1+\sqrt{5}}{2}$.

First, what do we even mean by convergence? We mean that the sequence of nested fractions truncated at level n

$$c_n=[a_0,a_1,\ldots,a_n]=a_0+\frac{1}{a_1+\frac{1}{a_2+\cdots+\frac{1}{a_n}}}$$

gives a converging sequence $(c_n)_{n\geq 1}$.

What are these partial convergents in the case of $[1,1,\ldots]$? Let's compute a few values

n	c_n
1	$\frac{3}{2}$
2	$\frac{5}{3}$
3	$\frac{8}{5}$
4	$\frac{13}{8}$.

We recognize these rational numbers as ratios of Fibonacci numbers. Let's make a guess:

$$c_n = \frac{F_{n+2}}{F_{n+1}},$$

and then check by induction that this is true. Then using the formula for the Fibonaccis we can compute that

$$\lim_{n\to\infty} c_n = \lim_{n\to\infty} \frac{F_{n+2}}{F_{n+1}} = \frac{1+\sqrt{5}}{2}.$$

Suppose now that you start with a real number, how would we go about finding its continued fraction expansion?

I worked out the example of e, first few digits. I also worked out $\frac{29}{13}$ and we noted that the process, and result, involve only quotients from the Euclidean algorithm. Ethan asked if this is unique, since fractions might not be in lowest terms, and we remarked that while the gcd and residues change if the fraction is not in lowest terms, the sequence of quotients does not.

Lecture 30
2022-11-07

Let's test our understanding of the notation of continued fractions.

1. First, we note that
$$[a_0, a_1, \ldots] = [a_0, a_1, \ldots, a_n, [a_{n+1}, \ldots]].$$

2. We also see, by inspection, that we can extend a finite continued fraction algorithmically:
$$[a_0, a_1, \ldots, a_n + x] = [a_0, a_1, \ldots, a_n, \frac{1}{x}].$$
As written, there is nothing unique about continued fractions expansions. Indeed,
$$e = [2 + e - 2] = [2, \frac{1}{e-2}]$$
$$e = [1 + e - 1] = [1, \frac{1}{e-1}]$$
are two different continued fractions. However, the coefficients of the continued fraction are, in both cases, still transcendental, and they don't reveal anything interesting about e.

3. The first entry can certainly be 0, as $\frac{1}{2} = [0, 2]$, but any other 0 entry can be suppressed:
$$[a_0, a_1, \ldots, a_n, 0, a_{n+1}, \ldots] = [a_0, a_1, \ldots, a_n + a_{n+1}, \ldots].$$

These observations allow us to restrict our attention to only positive integers (except for a_0), and for any

real number x, we can guarantee such an expansion as follows:

$$\begin{aligned} x = [x] &= [\underbrace{\lfloor x \rfloor}_{a_0} + \{x\}] \\ &= [a_0, \underbrace{\frac{1}{\{x\}}}_{x_1}] \\ &= [a_0, \underbrace{\lfloor x_1 \rfloor}_{a_1} + \{x_1\}] \\ &= [a_0, a_1, \underbrace{\frac{1}{\{x_1\}}}_{x_2}] \\ &\vdots \\ &= [a_0, a_1, \ldots, a_n, x_{n+1}] \end{aligned}$$

and so on. What's special about taking integer parts? The reason is that we want to be able to keep extending the process and only get positive integers. In this process, $a_n = \lfloor x_n \rfloor$ and $x_{n+1} = \frac{1}{\{x_n\}} \geq 1$.

5.1 Convergence

Let's only consider continued fractions

$$[a_0, a_1, \ldots]$$

where $a_1, a_2, \ldots \in \mathbb{Z}_{\geq 1}$. We'll prove that this continued fraction converges by showing that the sequence of partial convergents

$$c_n = [a_0, a_1, \ldots, a_n]$$

converge.

How to check convergence? If we knew what the limit is, we could verify that $\lim_{n\to\infty} c_n$ equals this limit. In the absence of a concrete real number that could plausibly be a limit (what could $[1, 2, 3, \ldots]$ possibly be as a real number?) the only notion that we have to verify convergence is that of a **Cauchy sequence**. We'll check that when $m, n \gg 0$, $|c_m - c_n|$ is small. In the real numbers, this Cauchy property guarantees convergence.

The huge problem is that (say $m > n$)

$$\begin{aligned} c_n &= [a_0, a_1, \ldots, a_n] \\ c_m &= [a_0, a_1, \ldots, a_n, \ldots a_m] \end{aligned}$$

are two nested fractions that are simply not comparable. How could we possibly check that $|c_m - c_n|$ is small?

Important trick

We'll use our previous properties of continued fractions to make them comparable:

$$\begin{aligned} c_n &= [a_0, a_1, \ldots, a_n] \\ &= [a_0, a_1, \ldots, a_n + 0] \\ &= [a_0, a_1, \ldots, a_n, \frac{1}{0}] \\ &= [a_0, a_1, \ldots, a_n, \infty] \end{aligned}$$

$$\begin{aligned} c_m &= [a_0, a_1, \ldots, a_n, \ldots a_m] \\ &= [a_0, a_1, \ldots, a_n, \underbrace{[a_{n+1}, \ldots a_m]}_{x}] \\ &= [a_0, a_1, \ldots, a_n, x] \end{aligned}$$

and the two expressions

$$\begin{aligned} c_n &= [a_0, a_1, \ldots, a_n, \infty] \\ c_m &= [a_0, a_1, \ldots, a_n, x] \end{aligned}$$

look very similar. They are both nested sequences of fractions, and their only difference occurs in the very last fraction. In fact, if we defined the function

$$f(x) = [a_0, a_1, \ldots, a_n, x]$$

the convergence question becomes a question about how small

$$|c_m - c_n| = |f(x) - f(\infty)|$$

is. We transformed an inscrutable question about far apart elements of a sequence into a calculus question about the range of a function $f(x)$.

In order to answer this question, let's get a feel for what $f(x)$ might look like.

Example 98. Consider $f(x) = [2, 4, 3, x]$. Then

$$\begin{aligned} f(x) &= 2 + \frac{1}{4 + \frac{1}{3 + \frac{1}{x}}} \\ &= 2 + \frac{1}{4 + \frac{x}{3x+1}} \\ &= 2 + \frac{3x+1}{13x+4} \\ &= \frac{29x+9}{13x+4}. \end{aligned}$$

It turns out, every $f(x)$ looks like this.

Definition 99. A **Mobius transformation** is a function of the form

$$f(x) = \frac{ax+b}{cx+d}.$$

It is not, technically, a function on $\mathbb{R}$, as it might have a vertical asymptote. However, using calculus, we can make sense of $f : \mathbb{R} \cup \{\infty\} \to \mathbb{R} \cup \{\infty\}$. By $f(\infty)$ we mean

$$f(\infty) = \lim_{x \to \infty} \frac{ax+b}{cx+d} = \frac{a}{c}.$$

If $x = -\frac{d}{c}$ the denominator vanishes and the formula doesn't, technically, make sense. Nonetheless, we define

$$f(-\frac{d}{c}) = \lim_{x \to -\frac{d}{c}} \frac{ax+b}{cx+d} \in \mathbb{R} \cup \{\infty\}.$$

Mobius transformation are in agreement with our understanding of continued fractions. Indeed, when $f(x) = [2, 4, 3, x]$ then

$$\begin{aligned} f(\infty) &= \frac{29}{13} \\ [2, 4, 3, \infty] = [2, 4, 3 + \frac{1}{\infty}] &= [2, 4, 3] = \frac{29}{13}. \end{aligned}$$

Lecture 31
2022-11-09

Remember our aim, to estimate $|f(x) - f(\infty)|$ when

$$f(x) = [a_0, a_1, \ldots, a_n, x]$$
$$x = [a_{n+1}, \ldots, a_m].$$

To do this, we need to compute the actual coefficients in $f(x) = \frac{ax+b}{cx+d}$.

Definition 100. Suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix with real entries, and $x \in \mathbb{R} \cup \{\infty\}$. We define

$$A \cdot x = \frac{ax + b}{cx + d}.$$

This operation is NOT matrix multiplication, as x is number, but it is not scalar multiplication either. You can think of $A \cdot x$ as a convenient way to denote the Mobius transformation $f(x) = \frac{ax+b}{cx+d}$. For convenience, we'll denote $f_A(x)$ the Mobius transformation $A \cdot x$.

The operation satisfies a marvelous associativity property, which is crucial for our approach to convergence.

Proposition 101. *If A and B are two matrices, and x is a scalar, then*

$$A \cdot (B \cdot x) = AB \cdot x.$$

What's going on here? Whenever we "dot" a matrix with a scalar, we get a scalar. So $B \cdot x$ is a scalar, and then we dot it with A. The point of this result is that we could have, equivalently, simply dotted x with the matrix product AB. Another way of writing this proposition is as follows: if $f_A \circ f_B = f_{AB}$. This is reminiscent of the result from linear algebra, that composing linear transformations is equivalent to multiplying their matrices, but this proposition is altogether different, as the functions are NOT linear transformations.

I wrote out the computation on the board.

What kind of function is the Mobius transformation $f_A(x) = A \cdot x$? We see that

$$\begin{aligned} f'_A(x) &= \frac{d}{dx}(A \cdot x) \\ &= \frac{ad - bc}{(cx + d)^2} \\ &= \frac{\det A}{(cx + d)^2}. \end{aligned}$$

This means that $f_A(x)$ never changes sign, and the monotonicity is entirely determined by $\det A$. This will be very convenient.

Proof of convergence of (c_n)

Before we can turn to the issue of convergence of the sequence (c_n), we need to determine what the Mobius transformation

$$f(x) = [a_0, a_1, \ldots, a_n, x]$$

looks like.

Lemma 102. *We have*

$$[a_0, a_1, \ldots, a_n, x] = [a_0, a_1, \ldots, a_{n-1}, \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdot x].$$

Moreover,

$$[a_0, a_1, \ldots, a_n, x] = \begin{pmatrix} a_0 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & \end{pmatrix} \cdot x.$$

Proof. I wrote it cleanly on the board, it's comes down to

$$[a_n, x] = [a_n + \frac{1}{x}] = [\begin{pmatrix} a_n & 1 \\ 1 & \end{pmatrix} \cdot x].$$

The second part comes by repeating the first part, and this is where the proposition on associativity is used. □

Finally, we can now show that $|c_m - c_n|$ is small if $m > n \gg 0$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & \end{pmatrix}.$$

Then, for $x = [a_{n+1}, \ldots, a_m]$ we have

$$\begin{aligned} |c_m - c_n| &= |f(x) - f(\infty)| \\ &= |\int_x^\infty f'(t)dt| \\ &= |\int_x^\infty \frac{\det A}{(ct+d)^2} dt|. \end{aligned}$$

What is $\det A$? It is $\prod \det \begin{pmatrix} a_k & 1 \\ 1 & \end{pmatrix} = (-1)^{n+1}$. This means that we can ignore it in the absolute value above and so

$$\begin{aligned} |c_m - c_n| &= |\int_x^\infty \frac{1}{(ct+d)^2} dt| \\ &= \int_0^\infty \frac{1}{(ct+d)^2} dt = \frac{1}{cd}. \end{aligned}$$

How to show that this is small? We simply need to show that c and d grow! Amazingly, c and d only depend on n, and not on m!

But look at the product

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & \end{pmatrix}.$$

Because on the RHS each a_k is positive and appears only once, once we multiply all the matrices, each of a, b, c, d will be an increasing linear function in each of the variables a_k.

To show that c, d grow as n grows, it's enough to show this in the situation when $a_0, a_1, \ldots, a_n$ are smallest possible, namely when they are all equal to 1. In this case,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}^{n+1}.$$

Where have we seen this matrix before? In computing the Fibonacci sequence!

We can try out a few examples, and then show by induction, that

$$\begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}^{n+1} = \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}$$

and it's clear that the bottom row entries grow to ∞, and in fact they grow exponentially fast to ∞, as we saw when we counted the number of digits of F_{10^6} early in the semester.

Lecture 32
2022-11-11

As we saw, the convergence of the sequence (c_n) is controlled by the matrices

$$A_n = \begin{pmatrix} a_0 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & \end{pmatrix}.$$

Let's try to understand these matrices.

Example 103. What are the matrices A_n when $c = [2, 4, 3, 1, \ldots]$. I worked it out at the board and noted that the 1st column of A_n is the same as the second column of A_{n+1}.

Let's denote

$$A_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}.$$

Some observations:

1. $\det A_n = (-1)^{n+1} = p_n q_{n-1} - p_{n-1} q_n$. This means that p_n and q_n are coprime, and we saw how this makes sense from properties of the determinant as well.
2. We also have
$$c_n = A_n \cdot \infty = \frac{p_n}{q_n},$$
which is a fraction already written in lowest terms.
3. Finally, $c_{n-1} = A_{n-1} \cdot \infty = A_n \cdot 0 = \frac{p_{n-1}}{q_{n-1}}$.

Back to understanding the convergence of (c_n). If n is odd, $\det A_n = 1$ and so $(A_n \cdot x)' = \frac{1}{(q_n x + q_{n-1})^2}$, meaning that $A_n \cdot x$ is increasing in x. But

$$\begin{aligned} c_{n-1} &= A_n \cdot 0 \\ c &= A_n \cdot [a_{n+1}, \ldots] \\ c_n &= A_n \cdot \infty \end{aligned}$$

so $c_{n-1} < c < c_n$. If n is even, the situation is reversed. This means that $c = [a_0, a_1, \ldots]$ is sandwiched between the even index partial convergents on the left, and the odd index partial convergents on the right.

What about $|c - c_n|$? Because of the squeeze, it must be that

$$|c - c_n| < |c_{n+1} - c_n| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Remark 18. What we achieved is a proof of the **Dirichlet approximation theorem**, that

$$|c - \frac{p}{q}| < \frac{1}{q^2}$$

whenever $p = p_n$ and $q = q_n$, so any real number c has excellent rational approximations.

This is the best result that can be, as the celebrated Thue-Roth-Siegel theorem implies that for any $\varepsilon > 0$ and any irrational algebraic number c you can find only finitely many rational $\frac{p}{q}$ such that

$$|c - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$$

These type of rational approximation results started with Liouville, who proved the above result with $2 + \varepsilon$ replaced with the degree of a polynomial whose root c is, to show that transcendental numbers exist. For instance,

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$

is approximated by the rational numbers $\displaystyle\sum_{n=0}^{m} \frac{1}{10^{n!}}$, but these approximations are so good, that they cannot be satisfied if α were algebraic.

Not only are the partial convergents $\frac{p_n}{q_n}$ excellent rational approximations of c, they are, in fact, the best possible rational approximations.

Theorem 104. *The partial convergent $\frac{p_n}{q_n}$ is the best possible rational approximation of c among all fractions whose denominator is at most q_n. In other words, if $0 < b \leq q_n$ then*

$$|c - \frac{p_n}{q_n}| \leq |c - \frac{a}{b}|$$

and equality can only occur when $\frac{a}{b} = \frac{p_n}{q_n}$.

Example 105. For $\pi = [3, 7, 15, 1, \ldots]$ has $c_1 = \frac{22}{7}$, $c_2 = \frac{333}{106}$, $c_3 = \frac{103993}{33102}$ and the theorem implies that $\frac{333}{106}$ is the best possible approximation of π using fractions with denominator ≤ 106.

Marie asked if we can see this in the case when $\frac{a}{b} = \frac{p_{n-1}}{q_{n-1}}$. This fantastic question gives us a glimpse on how to show the theorem.

Remember that

$$\begin{aligned} c_{n-1} &= A_n \cdot 0 \\ c &= A_n \cdot \underbrace{[a_{n+1}, \ldots]}_{x} \\ c_n &= A_n \cdot \infty \end{aligned}$$

so we'd like to show that

$$|A_n \cdot x - A_n \cdot 0| > |A_n \cdot \infty - A_n \cdot x|.$$

This inequality is NOT true for all values of x, just look at what happens when $x \to 0$. (In fact, $A_n \cdot x$ is a continuous function so $A_n \cdot x$ can be any number between $c_{n-1} = A_n \cdot 0$ and $c_n = A_n \cdot \infty$ by the intermediate value theorem.)

So let's figure out what extra we know about x.

$$x = [a_{n+1}, \ldots] = a_{n+1} + \frac{1}{\ldots} \geq a_{n+1} \geq 1.$$

So we'll now show that

$$|A_n \cdot x - A_n \cdot 0| > |A_n \cdot \infty - A_n \cdot x|,$$

whenever $x \geq 1$. Writing out the fractions, we'd have to check that

$$|\frac{(p_n q_{n-1} - p_{n-1} q_n)x}{q_{n-1}(q_n x + q_{n-1})}| > |\frac{p_n q_{n-1} - p_{n-1} q_n}{q_n(q_n x + q_{n-1})}|.$$

Simplifying, we'd have to check that

$$x > \frac{q_{n-1}}{q_n},$$

and this is true because (q_n) is an increasing sequence and so

$$x \geq 1 > \frac{q_{n-1}}{q_n}.$$

Aside on the Fibonacci sequences. I recalled that

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

I described as a black box from algebra that in a group G of order D, $g^D = 1$ for all $g \in G$, with parallels for $\mathbb{Z}_p^\times$ and $\mathbb{Z}_n^\times$. As an example, we took G to be the group of 2×2 matrices with entries in $\mathbb{Z}_p$ and determinant

$\not\equiv 0 \pmod{p}$. How many elements does this have? We need $\det \not\equiv 0$. We can achieve this by taking the first column of the 2×2 matrix to be not the 0 column, for a total of $p^2 - 1$ choices, and then the second column to be anything except a multiple of the first column, for a total of $p^2 - p$ choices. This means that G has $(p^2-1)(p^2-p)$ elements. Since $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in G$, we see that

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{(p^2-1)(p^2-p)} \equiv 1 \pmod{p}.$$

As a consequence, we saw that

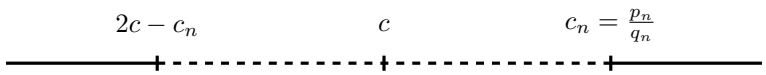
$$p \mid F_{(p^2-1)(p^2-p)}.$$

Lecture 33
2022-11-14

Proof of theorem. In class I presented the proof from the textbook. Here's another one, that's conceptually cleaner.

Let's work things out when n is odd, as the even case is identical.

Then $c < c_n = \frac{p_n}{q_n}$, which we can see because the function $A_n \cdot x$ is **increasing** and $c_n = A_n \cdot \infty$. In the picture below, c_n and $2c - c_n$ are symmetrical with respect to c, so we must show that $\frac{a}{b}$ is not in the dashed region. The trick is to ignore c itself, and show that $\frac{a}{b}$ can't be too close to c_n itself.



If $\frac{a}{b}$ were in the dashed part, it would have to be that

$$c_n - \frac{a}{b} < 2(c_n - c).$$

We'll derive a contradiction by bounding $c_n - c$ from above, and then $c_n - \frac{a}{b}$ from below.

First, we already saw that, as $A_n \cdot x$ is increasing,

$$\begin{aligned} c_n - c &= A_n \cdot \infty - A_n \cdot [a_{n+1}, \ldots] \\ &< A_n \cdot \infty - A_n \cdot 1 \\ &= \frac{1}{q_n(q_n + q_{n-1})}. \end{aligned}$$

At the same time, if $\frac{a}{b} \neq \frac{p_n}{q_n}$, it must be that (since $b \leq q_n$)

$$\begin{aligned} \frac{p_n}{q_n} - \frac{a}{b} &= \frac{p_n b - q_n a}{q_n b} \\ &\geq \frac{p_n b - q_n a}{q_n^2}. \end{aligned}$$

Therefore, it must be that

$$0 < p_n b - q_n a \leq \frac{2q_n}{q_n + q_{n-1}} < 2.$$

The only case we need to ignore is

$$p_n b - q_n a = 1.$$

For this, let's look at the equation

$$p_n x - q_n y = 1$$

with $x, y \in \mathbb{Z}$. We already know one solution, namely $x = q_{n-1}$ and $y = p_{n-1}$, coming from $\det A_n = 1$. We need to show that $x = b$, $y = a$ is not another solution. But, as $(p_n, q_n) = 1$, we know how to list all possible integer solutions:

$$x = q_{n-1} + q_n k$$
$$y = p_{n-1} + p_n k,$$

for integers k. We are asking if b can be of this form $b = q_{n-1} + q_n k$? Well, $b > 0$ and $b \leq q_n$, which together mean that $k = 0$. But the $\frac{a}{b} = \frac{p_{n-1}}{q_{n-1}}$, and we already know that this is farther from c than $\frac{p_n}{q_n}$. □

5.2 Rational numbers with lossy computations

We can now apply this to recovering rational numbers from floating point operations. Suppose we are given two decimal expansions: 0.4117647 and 0.4487989. Which of these is likely to be the 7-decimal approximation of a rational number?

Of course, this question is qualitative at best, since any finite decimal expansion is necessarily a rational number. What we want to answer is the following question: **Question:** Given a decimal expansion α with some number of digits, how close can a rational number be to α? If $\frac{p}{q}$ is much closer to α than the decimal approximation, and p and q are "small", we can conclude that α came from truncating the decimal expansion of $\frac{p}{q}$.

How do we tell rationals apart from irrationals using continued fractions? A number $c \in \mathbb{Q}$ iff its continued fraction is finite:

$$c = [a_0, a_1, \ldots, a_n].$$

But for any sequence of positive integers $a_{n+2}, \ldots$, we see that

$$c = [a_0, a_1, \ldots, a_n, \infty, a_{n+2}, \ldots].$$

So if we are given $c \in \mathbb{R}$, we can tell that it is rational if somewhere in its continued fraction we see ∞.

Example 106. Say $c_1 = 0.4117647$ and $c_2 = 0.4487989$. These numbers have finite decimals given, so they are rational and therefore have finite continued fractions expansions. What are they?

$$c_1 = [0, 2, 2, 3, \underbrace{588235}_{\text{huge}}]$$
$$c_2 = [0, 2, 4, 2, 1, 1, 1, 1, 2, 2, 17, 1, 1, 1, 1, 2, 10, 2, 2].$$

The fact that c_1 (in contrast with c_2) has a huge entry, namely 588235, it is plausible that this huge number should really be ∞, and would have been ∞ had we had infinitely many decimals. The second number doesn't have any huge entry, and we can't conclude plausibly that it comes from a rational number. In fact, it is the truncation of $\frac{\pi}{7}$. This doesn't mean that there is no plausible rational that could have the same 7 decimals. In fact, $\frac{355}{791}$ has the same 7 decimals as $\frac{pi}{7}$.

But let's get back to c_1. We guess that

$$c_1 \approx [0, 2, 2, 3, \infty] = \frac{p_3}{q_3} = \frac{7}{17}.$$

How close are the two numbers? We know that

$$|c_1 - \frac{7}{17}| < \frac{1}{q_3 q_4} = \frac{1}{q_3(q_3 a_4 + q_2)}.$$

Here

$$A_3 = \begin{pmatrix} 0 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 17 & 5 \end{pmatrix} = \begin{pmatrix} p_3 & p_2 \\ q_3 & q_2 \end{pmatrix}$$

so

$$|c_1 - \frac{7}{17}| < \frac{1}{17 \cdot (17 \cdot 588235 + 5)} = \frac{1}{17 \cdot 10^7} \approx 0.6 \cdot 10^{-8}.$$

Now what if we had decided that 17 is "huge" in the continued fraction expansion of c_2? We could have guesses that c_2 comes from $\frac{p_9}{q_9} = [0, 2, 4, 2, 1, 1, 1, 1, 2, 2] = \frac{355}{791}$. How close are they? In this case

$$A_9 = \begin{pmatrix} 355 & 149 \\ 791 & 332 \end{pmatrix}$$

so

$$|c_2 - \frac{355}{791}| < \frac{1}{791 \cdot (791 \cdot 17 + 332)} = \frac{1}{10899189} \approx 10^{-7}.$$

The difference is now clear: c_1 is approximated with a smaller fraction to better precision that c_2.

5.3 Quadratic continued fractions

Let's work out the continued fraction of $\sqrt{7}$.

$$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots],$$

which looks periodic. In fact, this is the case for all quadratics.

Theorem 107. *An irrational number has periodic continued fraction iff it is the root of a quadratic polynomial with integer coefficients.*

Remark 19. Period here means eventually periodic, as we already saw with $\sqrt{7}$. What kinds of numbers are completely periodic? The theorem tells us that they must be of the form $u + v\sqrt{D}$ for some rationals u, v. Galois showed that such reals have completely period continued fractions if and only if $u + v\sqrt{D} > 1$ and $0 > u - v\sqrt{D} > -1$ (the latter number is called the Galois conjugate of the first).

Example 108. Let's see how we could show that $\sqrt{7}$ has actually periodic continued fraction. We'll repeatedly use that $a + x = [a, \frac{1}{x}]$ and conjugation of fractions.

$$\begin{aligned}
\sqrt{7} &= [2, \frac{1}{\sqrt{7} - 2}] = [2, \frac{\sqrt{7} + 2}{3}] \\
&= [2, 1, \frac{3}{\sqrt{7} - 1}] = [2, 1, \frac{3(\sqrt{7} + 1)}{6}] = [2, 1, \frac{\sqrt{7} + 1}{2}] \\
&= [2, 1, 1, \frac{2}{\sqrt{7} - 1}] = [2, 1, 1, \frac{\sqrt{7} + 1}{3}] \\
&= [2, 1, 1, 1, \frac{3}{\sqrt{7} - 2}] = [2, 1, 1, 1, \sqrt{7} + 2] \\
&= [2, 1, 1, 1, 4, \frac{1}{\sqrt{7} - 2}] = [2, 1, 1, 1, 4, \frac{\sqrt{7} + 2}{3}]
\end{aligned}$$

and now we get repetition

$$\begin{aligned}
\sqrt{7} &= [2, \frac{\sqrt{7} + 2}{3}] \\
&= [2, 1, 1, 1, 4, \frac{\sqrt{7} + 2}{3}] \\
&= [2, 1, 1, 1, 4, 1, 1, 1, 4, \frac{\sqrt{7} + 2}{3}] \\
&\vdots \\
&= [2, \overline{1, 1, 1, 4}].
\end{aligned}$$

Proof of the theorem. Let's start with a completely periodic continued fraction. Say

$$x = [\overline{a_0, a_1, \ldots, a_n}].$$

Why is it quadratic? We use the same idea as in computing $\rho = [1, 1, \ldots]$:

$$x = [a_0, a_1, \ldots, a_n, x] = A_n \cdot x$$

so x must be a solution to an equation of the form $x = \frac{ax+b}{cx+d}$, and therefore quadratic.

What about an eventually periodic continued fraction? Say

$$x = [a_0, a_1, \ldots, a_n, \overline{b_1, \ldots, b_m}].$$

Then $[\overline{b_1, \ldots, b_m}] = u + v\sqrt{D}$ for some rational numbers u, v and

$$x = A_n \cdot (u + v\sqrt{D}) = \frac{a(u + v\sqrt{D}) + b}{c(u + v\sqrt{D}) + d}.$$

This is still of the form $U + V\sqrt{D}$, by conjugation.

Finally, we get to the reverse direction. Suppose we start with any quadratic irrational, of the form $u + v\sqrt{D}$ for some rational numbers u and v. How to show that the continued fraction is (eventually) periodic? This is tricky because the periods can be huge.

Let's take inspiration from our computation of the continued fraction of $\sqrt{7}$. What we observe is that at each stage, the last entry in the continued fraction is of the form $\frac{M+\sqrt{7}}{N}$ and the integer coefficients M, N are quite small. This is not an accident, we'll show that this is always true, and therefore we'll be able to use the same trick as in showing the periodicity of $F_n \pmod N$. Indeed, if M, N are bounded integers, there are only finitely many possibilities for the last entry $\frac{M+\sqrt{D}}{N}$ and therefore one such last entry must repeat, implying the periodicity of the continued fraction after this point.

Suppose we start with the quadratic irrational $\frac{M+\sqrt{D}}{N}$, where D is the discriminant (which need not be square-free). The case $\frac{M-\sqrt{D}}{N}$ is similar. Then at each stage we have

$$\frac{M + \sqrt{D}}{N} = [a_0, a_1, \ldots, a_n, \frac{M_n + \sqrt{D}}{N_n}].$$

Why is this true? We can compute what goes in $[a_0, a_1, \ldots, a_n, x]$ by solving

$$\frac{M + \sqrt{D}}{N} = A_n \cdot x$$

so

$$x = A_n^{-1} \cdot \frac{M + \sqrt{D}}{N},$$

and what we get is

$$x = \frac{(-1)^n(q_{n-1}M - p_{n-1}N)(q_nM - p_nN) + \sqrt{D}}{(q_nM - p_nN)^2 - q_n^2 D}.$$

Let's turn our attention to showing that M_n and N_n must be bounded from above. One can do this directly from the formulas above, but it's much cleaner to recall how we showed that partial convergents are excellent approximations. What we did is we used Mobius transformations, for whom variations could be measured with a simple integral.

Let's flip things around:

$$\frac{M+\sqrt{D}}{N} = A_n \cdot \frac{M_n+\sqrt{D}}{N_n}$$
$$A_n^{-1} \cdot \frac{M+\sqrt{D}}{N} = \frac{M_n+\sqrt{D}}{N_n}.$$

There doesn't seem to be any variation, the way we compared $A_n \cdot \infty$ and $A_n \cdot [a_{n+1}, \ldots]$. We only seem to have $\frac{M+\sqrt{D}}{N}$. This is where **Galois** comes into the picture. Remember that Galois gave a criterion for the complete periodicity of the continued fraction of $\frac{M+\sqrt{D}}{N}$ that involved the Galois conjugate $\frac{M-\sqrt{D}}{N}$ as well. Staring at formulas, or knowing that Galois conjugation is a field automorphism, we get the additional formula:

$$A_n^{-1} \cdot \frac{M+\sqrt{D}}{N} = \frac{M_n+\sqrt{D}}{N_n}$$
$$A_n^{-1} \cdot \frac{M-\sqrt{D}}{N} = \frac{M_n-\sqrt{D}}{N_n}.$$

and the variation we'll seek is between the two RHS. Indeed, the way we'll show that N_n is bounded is by showing that the two RHS, whose difference is $\frac{2\sqrt{D}}{N_n}$, can't be too small. We get

$$\begin{aligned}
\frac{2\sqrt{D}}{N_n} &= A_n^{-1} \cdot \frac{M+\sqrt{D}}{N} - A_n^{-1} \cdot \frac{M-\sqrt{D}}{N} \\
&= \int_{\frac{M-\sqrt{D}}{N}}^{\frac{M+\sqrt{D}}{N}} (A_n^{-1} \cdot t)' dt \\
&= (-1)^{n+1} \int_{\frac{M-\sqrt{D}}{N}}^{\frac{M+\sqrt{D}}{N}} \frac{dt}{(-q_n t + p_n)^2} \\
&= \frac{(-1)^n}{q_n^2} \left(\underbrace{\frac{1}{\frac{M+\sqrt{D}}{N} - \frac{p_n}{q_n}}}_{\text{goes to } 0} - \underbrace{\frac{1}{\frac{M-\sqrt{D}}{N} - \frac{p_n}{q_n}}}_{\text{does NOT go to } 0} \right).
\end{aligned}$$

Keep in mind that we want the RHS to not be too small. Look at the two denominators. The partial convergents $\frac{p_n}{q_n} \to \frac{M+\sqrt{D}}{N}$, so the second denominator is never close to 0, which means that the second fraction is bounded. We can ignore it because we divide it by q_n^2. Therefore as $n \to \infty$, and $|\frac{M+\sqrt{D}}{N} - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}}$, we see that

$$\frac{2\sqrt{D}}{N_n} \approx \frac{(-1)^n}{q_n^2} \frac{1}{\frac{M+\sqrt{D}}{N} - \frac{p_n}{q_n}} > \frac{q_{n+1}}{q_n} > 1.$$

This shows that N_n is bounded above.

What about an upper bound for M_n? If M_n were unbounded, so would be $r_n = \frac{M_n+\sqrt{D}}{N_n}$, as N_n is bounded. We already know that

$$|c - \frac{p_n}{q_n}| = \frac{1}{q_n(q_n r_n + q_{n-1})}$$

from when we showed the continued fractions converge. How to we show that r_n is bounded? It all comes down to the fact that

$$|c - \frac{p_n}{q_n}| > \frac{\text{const}}{q_n^2},$$

which immediately gives that r_n has to be bounded. This inequality is true not only for $\frac{p_n}{q_n}$, but for all fractions, which is Liouville's theorem. But let's just check it for this context, where we'll use again the idea of Galois conjugation.

$$\left|\left(\frac{M+\sqrt{D}}{N}-\frac{p_n}{q_n}\right)\left(\frac{M-\sqrt{D}}{N}-\frac{p_n}{q_n}\right)\right| = \left|\left(\frac{M}{N}-\frac{p_n}{q_n}\right)^2-\frac{D}{N^2}\right|$$
$$= \frac{\text{nonzero positive integer}}{N^2q_n^2}$$
$$\left|\underbrace{\left(\frac{M+\sqrt{D}}{N}-\frac{p_n}{q_n}\right)}_{\text{goes to } 0}\underbrace{\left(\frac{M-\sqrt{D}}{N}-\frac{p_n}{q_n}\right)}_{\text{goes to } \frac{2\sqrt{D}}{N}}\right| \geq \frac{1}{N^2q_n^2}$$
$$\left|\frac{M+\sqrt{D}}{N}-\frac{p_n}{q_n}\right| > \frac{\frac{1}{2\sqrt{D}N}-\varepsilon}{q_n^2}.$$

□

5.4 Quadratics with lossy computations

Showed how to use continued fractions to recognize rational and quadratic factors of polynomials with decimal approximations.

Lecture 35
2022-11-18

---

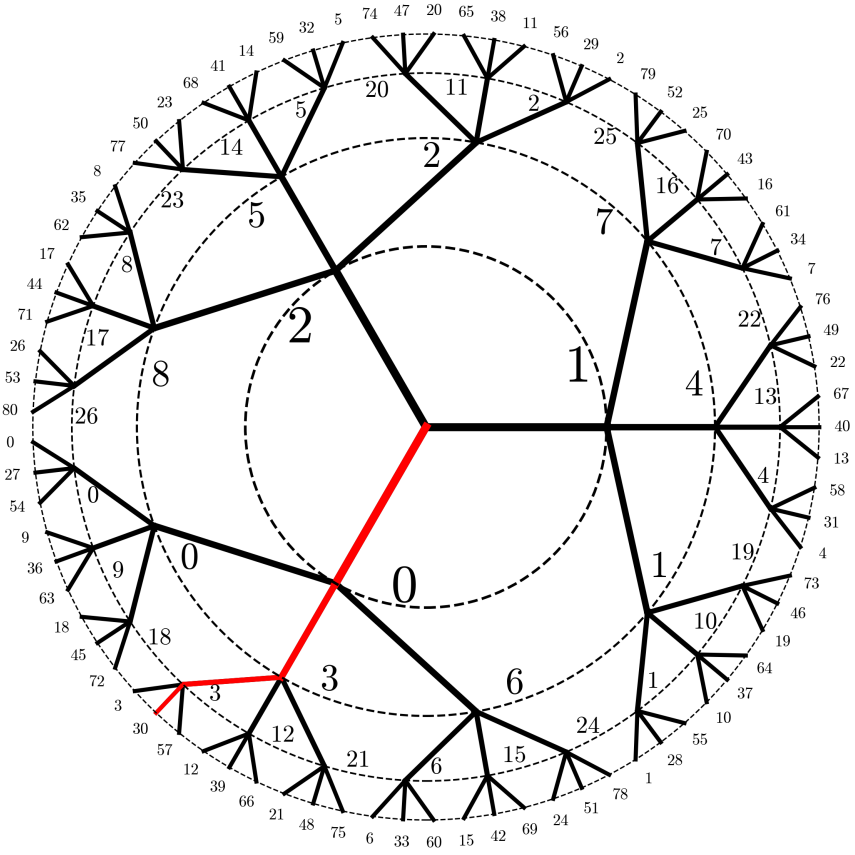
6 Polynomials modulo prime powers

Primitive roots modulo primes are special roots of $X^{\varphi(p^n)}-1 \pmod{p^n}$. In this section we address the issue of solving more general solutions modulo p^n.

Example 109. Determine all solutions of the equation $P(x)=x^3+x-57\equiv 0 \pmod{81}$.

By verifying every residue mod 81 we see that 30 is the unique solution. The key perspective is that if $P(a)\equiv 0 \pmod{p^n}$ then $P(a)\equiv 0 \pmod{p^k}$ for every $k<n$ as well. This means that 30 is a solution of $P(x)\equiv 0 \pmod{81}$, $30\equiv 3 \pmod{27}$ is a solution mod 27, 3 is a solution mod 9, $3\equiv 0 \pmod 3$ is a solution mod 3.

Let's organize all the residue classes mod 81, 27, 9, and 3 into a large tree as follows. The concentric circles contain all residues modulo 3^n, and a residue mod 3^n is connected by an edge to every residue mod 3^{n+1} to which it is congruent mod 3^n. In other words, $a \pmod{3^n}$ is connected with $a \pmod{3^{n+1}}$, $a+3^n \pmod{3^{n+1}}$ and $a+2\cdot 3^n \pmod{3^{n+1}}$. The red highlights are the roots of $P(x) \pmod{3^n}$.



The paradigm we will use is to flip the construction of the red ray. Rather than start with the solution 30 (mod 81) and obtain the ray, we will construct the ray one edge at a time, starting with $P(x) \equiv 0 \pmod 3$.

6.1 Hensel's lifting lemma

I recalled, in lecture, Newton's methods for approximating roots of functions.

Theorem 110 (Hensel's lifting lemma)**.** *Suppose $a \pmod p$ is a residue such that $P(a) \equiv 0 \pmod p$ and $P'(a) \not\equiv 0 \pmod p$. Let $x_1 = a$ and $x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)} \equiv x_n - \frac{P(x_n)}{P'(a)} \pmod{p^{n+1}}$. Then $P(x_n) \equiv 0 \pmod{p^n}$ for all n. Moreover, x_{n+1} is the ONLY solution of $P(x) \equiv 0 \pmod{p^{n+1}}$ such that $x_{n+1} \equiv x_n \pmod p$. In particular, x_n is the ONLY solution of $P(x) \equiv 0 \pmod{p^n}$ such that $x_n \equiv a \pmod p$.*

Proof. I worked out the proof in class, using the Taylor expansion of $P(x)$ around x_n. □

Example 111. Returning to our example $x^3 + x - 57 \equiv 0 \pmod{81}$, we start with $P(x) \equiv 0 \pmod 3$. The only solution is $x \equiv 0 \pmod 3$, and we remark that $P'(x) = 3x^2 + 1$ so $P'(0) \not\equiv 0 \pmod 3$. We compute

$$\begin{aligned} x_1 &\equiv 0 \pmod 3 \\ x_2 &\equiv x_1 - \frac{P(x_1)}{P'(0)} \equiv 3 \pmod 9 \\ x_3 &\equiv x_2 - \frac{P(x_2)}{P'(0)} \equiv 3 \pmod{27} \\ x_4 &\equiv x_3 - \frac{P(x_3)}{P'(0)} \equiv 30 \pmod{81}. \end{aligned}$$

We recovered the solution 30 (mod 81), but in fact much more. Simply by starting with the unique solution 0 (mod 3), the fact that the derivative didn't vanish mod 3 implied that 30 is the UNIQUE solution mod 81. Moreover, the equation has a unique solution modulo all powers of 3, and the algorithm in Hensel's lifting lemma is very fast. For instance, very quickly we get that the only solution mod 3^{20} is 1162785648.

Lecture 36
2022-11-21

Remark 20. Hensel's lemma is extremely effective computationally, but it is most useful to show the existence and uniqueness of solutions modulo prime powers. However, Hensel's lemma is about lifting roots mod p to p^n, which means that we must first answer the question of roots mod p.

Example 112. Suppose a is an odd integer. Then $x^2 \equiv a \pmod{2^n}$ has solutions modulo all n if and only if $a \equiv 1 \pmod 8$. In particular, $x^2 \equiv 17 \pmod{2^n}$ has solutions modulo all powers of 2.

It's easy to check that 1 (mod 8) are the only odd quadratic residues mod 8. To see the reverse, suppose $a = 8k + 1$. It's tricky to apply Hensel's lemma because $P(x) = x^2 - a$ always has $P'(x) \equiv 0 \pmod 2$. Instead, any solution to $x^2 \equiv a \pmod{2^n}$ will have to be odd, so let's write $x = 2y + 1$. We're solving

$$x^2 - a = (2y + 1)^2 - (8k + 1) = 4(y^2 + y - 2k) \equiv 0 \pmod{2^n}.$$

To show that this has solutions, it's certainly enough to show that $y^2 + y - 2k \equiv 0 \pmod{2^n}$ has solutions. But $Q(y) = y^2 + y - 2k$ has $Q(0) \equiv 0 \pmod 2$ and $Q'(0) \equiv 1 \pmod 2$ so Hensel's lemma immediately implies the existence of a unique solution modulo 2^n with $y \equiv 0 \pmod 2$. But the quadratic $x^2 \equiv a \pmod{2^n}$ surely has another solution, the negative of the original one. Where did this one disappear? Nowhere! We see that $Q(1) \equiv 0 \pmod 2$ and $Q'(1) \equiv 1 \pmod 2$ so there again a unique solution mod 2^n which is 1 (mod 2).

The following compelling example shows that equations can have solutions mod all integers without having any integer solutions.

Example 113. The equation $2x^2 + 7y^2 = 1$ has the solution $(\frac{1}{3}, \frac{1}{3})$, but it has no integer solutions. Nonetheless, it has solutions mod all positive integers.

By CRT we only need to show that $2x^2 + 7y^2 \equiv 1 \pmod{p^n}$ has solutions mod all prime powers. First of all, if $p \neq 3$, then $x = y = 3^{-1} \pmod{p^n}$ will work! Let's show that $2x^2 + 7y^2 \equiv 1 \pmod{3^n}$ has solutions. We'll use Hensel, and start with $2x^2 + 7y^2 \equiv 2x^2 + y^2 \equiv 1 \pmod 3$. The problem is, of course, that Hensel is about single variable polynomials, not 2 variable ones. This just means that we have to fix one variable.

By inspection, one solution is $x = 0$, $y = 1$. We could try $P(x) = 2x^2 + 1^2 - 1$ or $Q(y) = 2 \cdot 0^2 + y^2 - 1$ and see which one gives solutions mod 3^n. But $P'(0) = 0$ so that's no good. However, $Q(1) \equiv 0 \pmod 3$ and $Q'(1) \equiv 2 \pmod 3$ so Hensel implies the existence of solutions of the form $(0, y)$ mod 3^n.

Lecture 37
2022-11-28

6.2 The local-global principle

Last week, we saw the example of the equation $2x^2 + 7y^2 = 1$ with no integer solutions, but with solutions modulo every N, which we obtain using a rational solution. We can reformulate this example entirely in terms of integers, by clearing denominators. If $x = X/Z$ and $y = Y/Z$ the equation becomes $2X^2 + 7Y^2 = Z^2$, with integer solution $(1, 1, 3)$. Any integer solution with $Z \neq 0$ yields a rational solution of the original equation.

The following consequential results in number theory states that this example is indicative of a general phenomenon, referred to as the local-global principle, for reasons having to do with p-adic numbers.

Theorem 114 (Hasse-Minkowski)**.** *Suppose $Q(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ is a homogeneous quadratic polynomial, i.e., every monomial in Q is of the form ax_ix_j. Then $Q(x_1, \ldots, x_n)$ has some non-zero integer solution if and only if:*

1. *$Q(x_1, \ldots, x_n)$ has a nonzero real solution AND*
2. *$Q(x_1, \ldots, x_n) \equiv 0 \pmod{N}$ has a nonzero solution modulo every integer N. Equivalently, it has solutions modulo prime powers, by CRT.*

Example 115. Let's show that $x^2 + y^2 = 2017$ has rational solutions. By clearing denominators we get

$$x^2 + y^2 = 2017z^2.$$

Hasse-Minkowski allows us to verify the existence of real solutions, and solutions mod prime powers. First, the real solutions form a cone, so there are nonzero real solutions.

What about prime powers? Let's work out a few examples. In fact, in all the cases below we'll use $z = 1$.

1. $p = 2$. Does $x^2 + y^2 \equiv 2017 \pmod{2^n}$ have solutions? Sure, already $x^2 + 0 \equiv 2017 \pmod{2^n}$ has solutions as $2017 \equiv 1 \pmod 8$.
2. $p = 3$. Again, $x^2 + 0 \equiv 2017 \pmod{3^n}$ will have solutions, by starting with $x = 1 \pmod 3$ and then use Hensel's lemma, the derivative being 2.
3. $p = 5$ so $x^2 + y^2 \equiv 2017 \pmod{5^n}$. Mod 5 a simple solution is $x = y = 1$. Then Hensel works to show that $x^2 + 1^2 \equiv 2017 \pmod{5^n}$ as the derivative will then be 2.
4. There's a special prime $p = 2017$. Now we need to check if $x^2 + y^2 \equiv 0 \pmod{p^n}$ has solutions. Does $x^2 + y^2 \equiv 0 \pmod p$ have a solution? Whatever solution we get, to lift it with Hensel we'd need the derivative $2x$ or $2y$ to be nonzero, so we could divide and try to solve $(x/y)^2 \equiv -1 \pmod p$. Does this have a solution? Sure, because $p \equiv 1 \pmod 4$ and so $\left(\frac{-1}{p}\right) = 1$.
5. Let's try general odd $p \neq 2017$. Hensel would guarantee the existence of solutions mod p^n if we start with ANY solution $x^2 + y^2 \equiv 2017 \pmod p$ with x or y nonzero. (Actually, because $p \neq 2017$, x and y can't both be 0, so this condition is automatic.) How would we solve this equation? It helps to switch perspective: what we want is to show that $x^2 \equiv 2017 - y^2 \pmod p$ has SOME solution.

   We could try to show that for some y, $2017 - y^2$ is a quadratic residue mod p, so $\left(\frac{2017-y^2}{p}\right) = 1$ for some y. In fact, one could show that $\sum \left(\frac{2017-y^2}{p}\right) \equiv \left(\frac{-1}{p}\right) \equiv 1 \pmod p$, so for some y the symbol is not 0. But this is an overkill. Half of the elements of $\mathbb{Z}_p^\times$ are quadratic residues. Including 0, this means $\frac{p+1}{2}$ values taken by x^2, and $\frac{p+1}{2}$ values for $2017 - y^2$. Since there are only p residues in total, these two sets of $\frac{p+1}{2}$ residues cannot be disjoint, so for SOME x and y it must be that $x^2 \equiv 2017 - y^2 \pmod p$.

6.3 Rational points on conics

Hasse-Minkowski gives a concrete algorithm for determining if a quadratic curve (a conic) has some rational solution. In this section we'll use this one solution to determine every rational solution. This procedure yields a parametrization of all rational points on any conic AS LONG AS we are given one rational point.

The most classical example is the circle $x^2 + y^2 = 1$. Clearing denominators, rational solution $x = X/Z$ and $y = Y/Z$ correspond to pythagorean triples $X^2 + Y^2 = Z^2$.

Proposition 116. *Up to swapping X and Y, every pythagorean triple is of the form*

$$\begin{aligned} X &= (m^2 - n^2)d \\ Y &= 2mnd \\ Z &= (m^2 + n^2)d. \end{aligned}$$

Proof. Dividing by Z^2, this is equivalent to finding rational solutions to $x^2 + y^2 = 1$. We'll start with one solution $(1, 0)$ (though any other rational solution will work, and in class I chose $(0, 1)$).

The trick is that finding all (x, y) rational on the circle is hard because there are two variables to compute. However, every point (x, y) on the circle yields a single line through (x, y) and the original chosen solution $(1, 0)$. A single line through a fixed point, $(1, 0)$ in this case, is uniquely determined by its slope. Say t is the slope. (In class t was the x-coordinate of the intersection of the line $(x, y)(0, 1)$ with the x-axis. Slightly different, but equivalent.)

What does this mean in terms of formulas?

$$t = \frac{y}{x - 1}.$$

If (x, y) is a rational solution, it follows that t must be rational as well. Let's go in the other direction, start with a rational t and solve for x and y. This will parametrize all rational solutions.

We know that $y = t(x-1)$ from the slope formula, and we know the circle equation $x^2+y^2 = 1$. Plugging in, we get

$$\begin{aligned} x^2 + y^2 &= 1 \\ x^2 + t^2(x-1)^2 &= 1 \\ x^2(t^2+1) - 2t^2x + t^2 - 1 &= 0. \end{aligned}$$

It's now enough to solve this quadratic equation. Actually, we'll cheat. We know that the two roots of any quadratic $ax^2 + bx + c = 0$ add up to $-b/a$, so if you know one root, you know the other as well.

In this case, we know the original rational point $(1, 0)$, so $x = 1$ must be a root of the quadratic. What about the other root x? It must be the case that

$$\underbrace{1}_{\text{root 1}} + \underbrace{x}_{\text{root 2}} = -\frac{-2t^2}{t^2+1},$$

so $x = \dfrac{t^2-1}{t^2+1}$. Then $y = t(x-1) = \dfrac{2t}{t^2+1}$.

What does this have to do with pythagorean triples? Writing $t = \frac{m}{n}$ gives $x = \frac{X}{Z} = \frac{m^2-n^2}{m^2+n^2}$ and $y = \frac{Y}{Z} = \frac{2mn}{m^2+n^2}$. □

This procedure works for all conics because in any quadratic, if you know one root (such as one coming from an initial chosen rational point), you know the other root as well easily.

Example 117. Find all rational roots of $x^2 - 5xy - 2y^2 = -17$. This conic is a hyperbola, and it has the rational point $(1, 2)$. Let's find all other rational points (x, y).

Again, let t be the slope of the line through $(1, 2)$ and (x, y), so

$$t = \frac{y-2}{x-1},$$

which means $y = 2 + t(x - 1)$. Again, if the point (x, y) is rational, so is t, so we start with an arbitrary rational t and try to solve for x and y.

Plugging in, we get

$$\begin{aligned} x^2 - 5xy - 2y^2 &= -17 \\ x^2 - 5x(2 + t(x-1)) - 2(2 + t(x-1))^2 &= -17 \\ x^2(1 - 5t - 2t^2) + x(4t^2 - 3t - 10) - 2t^2 + 8t - 8 &= -17. \end{aligned}$$

The two roots, 1 (from the chose point $(1,2)$) and x, must add up to

$$1+x=-\frac{4t^2-3t-10}{1-5t-2t^2},$$

which gives

$$\begin{aligned} x&=\frac{4t^2-3t-10}{2t^2+5t-1}-1\\ y&=2+t(x-1). \end{aligned}$$

Pick ANY rational t and plug it into these formulas, and you'll get a rational point on the hyperbola. For instance, picking $t=\frac{3}{5}$, we get $x=-\frac{327}{68}$ and $y=-\frac{101}{68}$.

Lecture 38
2022-11-30

---

7 The Riemann ζ-function

The Riemann zeta function

$$\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

is one of the most important functions in math. (It is related to the most important one, namely e^{-x^2}.)

When does it converge? How to check? The integral test gives that $\zeta(s)\approx\int_1^\infty\frac{dx}{x^s}=\frac{1}{s-1}$. Why does this approximation give convergence? Drawing the graph, the curve $y=\frac{1}{x^s}$ lies above all the right Riemann rectangles, so

$$\zeta(s)=1+\sum_{n=2}^{\infty}\frac{1}{n^s}<1+\int_1^\infty\frac{dx}{x^s}=1+\frac{1}{s-1},$$

so the series converges (absolutely) whenever $s>1$. It has a vertical asymptote at $s=1$, for instance because the left Riemann rectangles lie above the graph. How well does the integral control the vertical asymptote of $\zeta(s)$? I explained in class that

$$\zeta(s)-\frac{1}{s-1}=\zeta(s)-\int_1^\infty\frac{dx}{x^s}$$

is the area between the graph and the Riemann rectangles. If $s>0$ this error area converges because already the area between the left and right Riemann rectangles is a telescopic sum which evaluates to 1. So

$$\zeta(s)=\frac{1}{s-1}+\text{a function which converges absolutely when } s>0.$$

Theorem 118. *We have*

$$\begin{aligned} \zeta(2)&=\frac{\pi^2}{6}\\ \zeta(4)&=\frac{\pi^4}{90}\\ \zeta(2k)&=\mathit{rational}\cdot\pi^{2k}. \end{aligned}$$

Proof. It all starts with the function $\cot(x)$. I drew the graph, and the Laurent expansion

$$\cot(x)=\frac{1}{x}-\frac{x}{3}-\frac{x^3}{45}\cdots.$$

The cot function has poles precisely at $n\pi$ where $n \in \mathbb{Z}$. Much like partial fractions can expand a rational function into a simple sum whose denominators involve the poles, one has

$$\cot(x) = \frac{1}{x} + \frac{1}{x-\pi} + \frac{1}{x+\pi} + \frac{1}{x-2\pi} + \frac{1}{x+2\pi} + \cdots .$$

There are many ways to show this, but the best methods use complex analysis. One layer of difficulty is that, as written, the expansion on the RHS does not converge. To make things convergent, one needs to group fractions into pairs:

$$\cot(x) = \frac{1}{x} + \sum_{n=1}^{\infty} \left(\frac{1}{x-n\pi} + \frac{1}{x+n\pi} \right) = \frac{1}{x} + \sum_{n=1}^{\infty} \frac{2x}{x^2 - n^2\pi^2}.$$

Let's put things together

$$\begin{aligned} \frac{1}{x} - \frac{x}{3} - \frac{x^3}{45} \cdots = \cot(x) &= \frac{1}{x} + \sum_{n=1}^{\infty} \frac{2x}{x^2 - n^2\pi^2} \\ -\frac{x}{3} - \frac{x^3}{45} \cdots &= \sum_{n=1}^{\infty} \frac{2x}{x^2 - n^2\pi^2}. \end{aligned}$$

Dividing by $-2x$ we get

$$\frac{1}{6} + \frac{x^2}{90} \cdots = \sum_{n=1}^{\infty} \frac{1}{n^2\pi^2 - x^2}.$$

To get something useful, we need to rewrite the fractions on the RHS as power series in x, as on the LHS. I explained how to use the geometric series:

$$\begin{aligned} \frac{1}{6} + \frac{x^2}{90} \cdots &= \sum_{n=1}^{\infty} \frac{1}{n^2\pi^2} \cdot \frac{1}{1 - \frac{x^2}{n^2\pi^2}} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^2\pi^2} \cdot \left(1 + \frac{x^2}{n^2\pi^2} + \frac{x^4}{n^4\pi^4} + \cdots \right). \end{aligned}$$

Now simply equate coefficients. Comparing constant coefficients we get

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{1}{n^2\pi^2} &= \frac{1}{6} \\ \zeta(2) &= \frac{\pi^2}{6}. \end{aligned}$$

Comparing the coefficients of x^2 we get

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{1}{n^4\pi^4} &= \frac{1}{90} \\ \zeta(4) &= \frac{\pi^4}{90}. \end{aligned}$$

In general, comparing the coefficients of x^{2k} we get that $\zeta(2k)$ is π^{2k} times a Laurent coefficient of $\cot(x)$, all of which are rational, because these coefficients involve only factorials and evaluating trig functions at 0 after applying the quotient rule many times. □

Theorem 119 (Euler product)**.** *If $s > 1$,*

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}} = \frac{1}{1 - \frac{1}{2^s}} \frac{1}{1 - \frac{1}{3^s}} \frac{1}{1 - \frac{1}{5^s}} \cdots .$$

Example 120. Let's see how we can use the Euler product to gain information about asymptotic counts, such as

$$\text{number of square-free integers} \leq X \approx \frac{6}{\pi^2} X$$
$$\text{number of positive distinct fractions with numerator and denominator} \leq X \approx \frac{6}{\pi^2} X^2.$$

Let's try a (problematic) probabilistic approach to the first count. For a random integer n to be square-free, it needs to not be a multiple of any square of a prime. If "random integer" were a genuine random variable (which it cannot be for formal reasons) then the events $p^2 \nmid n$ would be independent (by CRT). Therefore

$$\begin{aligned} \Pr(2^2 \nmid n, 3^2 \nmid n, \ldots) &= \prod_p \Pr(p^2 \nmid n) \\ &= \prod_p \left(1 - \Pr(p^2 \mid n)\right) \\ &= \prod_p \left(1 - \frac{1}{p^2}\right) \\ &= \frac{1}{\zeta(2)} = \frac{6}{\pi^2}. \end{aligned}$$

Of course, this is problematic because "random integer" is. We'll make sense of a probability density measure that is rigorous next lecture.

Lecture 39
2022-12-02

I proved the Euler product result, using unique factorization of integers.

Example 121. Compute

$$\sum_{n \text{ square-free}} \frac{1}{n^2}.$$

By the same method, we see that

$$\begin{aligned} \sum_{n \text{ square-free}} \frac{1}{n^2} &= \prod_p \left(1 + \frac{1}{p^2}\right) \\ &= \prod_p \frac{1 - \frac{1}{p^4}}{1 - \frac{1}{p^2}} \\ &= \frac{\zeta(2)}{\zeta(4)} = \frac{\frac{\pi^2}{6}}{\frac{\pi^4}{90}} \\ &= \frac{15}{\pi^2}. \end{aligned}$$

A fantastic application of the Euler product is the following:

Lemma 122.

$$\sum_p \frac{1}{p} = \infty.$$

Proof. If $s > 1$

$$\begin{aligned}\ln \zeta(s) &= -\sum \ln\left(1 - \frac{1}{p^s}\right) \\ &\approx \sum_p \frac{1}{p^s},\end{aligned}$$

the error being at most $\sum_p \frac{1}{p^{2s}}$, which converges whenever $s > \frac{1}{2}$. In particular, the error is bounded as $s \to 1$. This means that as $s \to 1^+$, we have

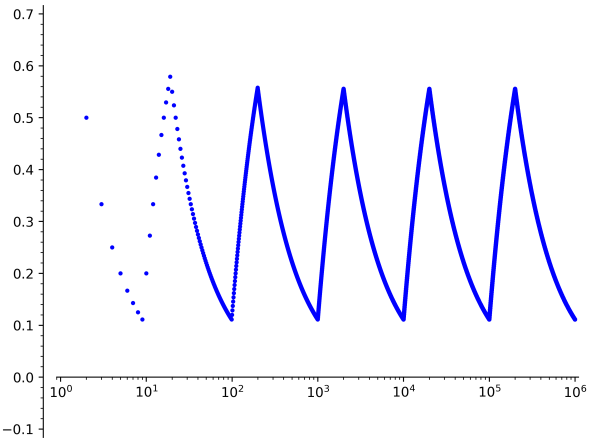
$$\sum_p \frac{1}{p^s} \approx \ln \zeta(s) \approx \ln \frac{1}{s-1}$$

so $\sum \frac{1}{p}$ diverges. □

7.1 Density

In attempting to count square-free integers, we ran into problems, because "random integer" is not meaningful. Dirichlet came up with an ingenious work-around, by estimating "density" rather than "probability".

Example 123. What is the likelihood that a positive integer starts with the digits 1? Intuitively, it should be $\frac{1}{9}$. How would we quantify this intuition? One option is to count how many integers up to some bound start with 1. For instance, up to 999 there are 111 numbers that start with 1, so it looks like we get $\frac{1}{9}$. But if we stop our count at 200, then the proportion is $\frac{111}{200}$. In fact, if we plot the proportion of positive integers that start with 1 up to N as a function of N we get



The proportion, as $N \to \infty$, does not converge.

The previous example suggests that the naive measure of proportion is not fine enough to capture our intuition. A different notion of density is needed. The fundamental problem is that "density" is very sensitive to how we count integers.

To circumvent problematic counting strategies, Dirichlet's idea is to measure density not via counting up to X, but by considering all positive integers at the same time, using the Riemann ζ-function. For instance, intuition tells us that exactly $\frac{1}{5}$ of integers are multiples of 5, and we can see this already using counting

arguments: precisely $\lfloor \frac{X}{5} \rfloor$ of integers up to X are multiple of 5. How would this work using $\zeta(s)$? Let's compare

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$
$$D_{\text{multiple of } 5}(s) = \sum_{n \geq 1, 5|n} \frac{1}{n^s}.$$

Since $\zeta(s)$ is completely dominated by $\frac{1}{s-1}$ as $s \to 1^+$, its asymptotic behavious around 1 ignores hard-to-control errors. What about the second series? We see that

$$D_{\text{multiple of } 5}(s) = \frac{1}{5^s}\zeta(s)$$

so around $s \to 1^+$ we have

$$D_{\text{multiple of } 5}(s) \approx \frac{1}{5} \cdot \frac{1}{s-1}.$$

Dirichlet noted that our intuitive guess of density $\frac{1}{5}$ is confirmed by

$$\frac{1}{5} = \lim_{s \to 1^+} \frac{D_{\text{multiple of } 5}(s)}{\zeta(s)}.$$

Definition 124. Suppose $\mathcal{A} \subset \mathcal{B}$ are two sets of integers. The Dirichlet density of $\mathcal{A}$ relative to $\mathcal{B}$ is

$$\lim_{s \to 1^+} \frac{\sum_{n \in \mathcal{A}} \frac{1}{n^s}}{\sum_{n \in \mathcal{B}} \frac{1}{n^s}},$$

if it exists. Typically, we estimate the Dirichlet density of a set of integers relative to all integers, or the Dirichlet density of a set of primes relative to all primes.

We can now make formal our intution about square-free integers.

Lemma 125. *The Dirichlet density of square-free integers (relative to all positive integers) is* $\frac{6}{\pi^2}$.

Proof. Indeed,

$$\sum_{n \text{ square-free}} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s}\right)$$
$$= \frac{\zeta(s)}{\zeta(2s)},$$

so the Dirichlet density is

$$\lim_{s \to 1^+} \frac{\sum_{n \text{ square-free}} \frac{1}{n^s}}{\zeta(s)} = \lim_{s \to 1^+} \frac{1}{\zeta(2s)} = \frac{1}{\zeta(2)}.$$

□

Example 126. Back to our example with integers that start with 1. Let's rewrite the Dirichlet series in terms of numbers of digits:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{d=0}^{\infty} \sum_{m=0}^{9 \cdot 10^d - 1} \frac{1}{(10^d + m)^s}$$
$$\sum_{n=1, n=1abc\ldots}^{\infty} \frac{1}{n^s} = \sum_{d=0}^{\infty} \sum_{m=0}^{10^d - 1} \frac{1}{(10^d + m)^s}$$

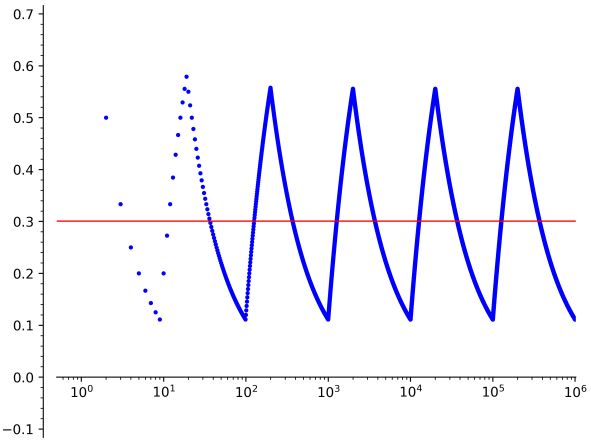
Let's estimate their asymptotic behaviors. In the following computations, a can be 1 or 9. One needs to be careful about errors in using integrals to approximate Riemann sums, but in the limit the errors don't matter.

$$\begin{aligned}\sum_{d=0}^{\infty}\sum_{m=0}^{a\cdot 10^d-1}\frac{1}{(10^d+m)^s} &= \sum_{d=0}^{\infty}\frac{1}{10^{d(s-1)}}\left(\frac{1}{10^d}\sum_{m=0}^{a\cdot 10^d-1}\frac{1}{(1+\frac{m}{10^d})^s}\right)\\ &\approx \sum_{d=0}^{\infty}\frac{1}{10^{d(s-1)}}\int_0^a\frac{dx}{(1+x)^s}\\ &= \frac{1}{1-\frac{1}{10^{s-1}}}\int_0^a\frac{dx}{(1+x)^s}.\end{aligned}$$

Computing Dirichlet density we see

$$\begin{aligned}\lim_{s\to 1^+}\frac{\sum_{n=1abc\ldots}\frac{1}{n^s}}{\sum_{n\geq 1}\frac{1}{n^s}} &= \lim_{s\to 1^+}\frac{\frac{1}{1-\frac{1}{10^{s-1}}}\int_0^1\frac{dx}{(1+x)^s}}{\frac{1}{1-\frac{1}{10^{s-1}}}\int_0^9\frac{dx}{(1+x)^s}}\\ &= \frac{\int_0^1\frac{dx}{1+x}}{\int_0^9\frac{dx}{1+x}} = \frac{\ln(2)}{\ln(10)}.\end{aligned}$$

This answer confounds our intuition! One interpretation is that the Dirichlet density is an average of the naive density asymptotically.



This density $\frac{\ln(2)}{\ln(10)}$ is also the Dirichlet density of primes that begin with the digit 1 (I got this example from Serre "A Course in Arithmetic" §4.5), as well as the proportion of integers n for which 2^n (or 3^n, etc) begins with the digit 1.

We'll finish with a special case of Dirichlet's theorem on primes in arithmetic progressions. We already established that there are infinitely many primes $\equiv 1 \pmod 4$ (resp. $\equiv 3 \pmod 4$).

Theorem 127 (Dirichlet)**.** *The set of primes* $\equiv 1 \pmod 4$ *(resp.* $\equiv 3 \pmod 4$*) has Dirichlet density* $\frac{1}{2}$*.*

Proof. In other words, we'll have to show that

$$\lim_{s\to 1^+}\frac{\sum_{p\equiv 1 \pmod 4}\frac{1}{p^s}}{\sum_p\frac{1}{p^s}} = \frac{1}{2}.$$

Just like when we first looked at $\sum \frac{1}{p^s}$, by estimating $\ln \zeta(s)$, we'll start approximating the numerator by looking at a Dirichlet series.

Let $A(s) = \sum_{2\nmid n} \frac{n \mod 4}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots$. The Dirichlet series $A(s)$ has an Euler product

$$\begin{aligned} A(s) &= \prod_{p>2} \frac{1}{1 - \frac{p \mod 4}{p^s}} \\ \ln A(s) &\approx \sum_{p>2} \frac{p \mod 4}{p^s}, \end{aligned}$$

the error in the approximation again bounded as $s \to 1^+$.

Now comes a trick:

$$\begin{aligned} \sum_{p \equiv 1 \pmod 4} \frac{1}{p^s} &= \sum_p \frac{1}{2} \left(\frac{1}{p^s} + \frac{p \mod 4}{p^s} \right) \\ &\approx \frac{1}{2} \left(\ln \zeta(s) + \ln A(s) \right). \end{aligned}$$

We're now ready to compute the density of primes $\equiv 1 \pmod 4$. We have

$$\begin{aligned} \lim_{s \to 1^+} \frac{\sum_{p \equiv 1 \pmod 4} \frac{1}{p^s}}{\sum_p \frac{1}{p^s}} &= \lim_{s \to 1^+} \frac{\frac{1}{2}(\ln \zeta(s) + \ln A(s))}{\ln \zeta(s)} \\ &= \frac{1}{2} + \lim_{s \to 1^+} \frac{A(s)}{2 \ln \zeta(s)} \\ &= \frac{1}{2} + \frac{\ln \frac{\pi}{4}}{\infty} = \frac{1}{2}. \end{aligned}$$

□

Lecture 40
2022-12-05

Primality testing and probabilistic models of primes.

Lecture 41
2022-12-07

Primality testing and probabilistic models of primes.