Math 43900 Problem Solving
Fall 2021
Lecture 7 Number Theory

Andrei Jorza Evan O'Dorney

These problems are taken from the textbook, from Engel's *Problem solving strategies*, from Ravi Vakil's Putnam seminar notes and from Po-Shen Loh's Putnam seminar notes.

Number Theory

There are three main themes that show up in competition-style number-theory-related problems: modular arithmetic, Diophantine equations and divisibility. There's lots of other themes and ideas, such as infinite descent, integral functions and inequalities: you can see lots of these ideas in the textbook. Number theory is too vast and diverse to capture in one lecture or one collection of a dozen exercises, especially when it is combined with combinatorics. My best suggestion is to try to get a feel for what's out there from the examples and exercises in the textbook.

Some useful facts are:

1. Modular arithmetic: Suppose that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then

$$a + c \equiv b + d, \quad a - c \equiv b - d, \quad ac \equiv bd \mod m.$$

   If c is invertible modulo m (that is, $\gcd(c, m) = 1$, then also $a/c \equiv b/d \bmod m$. More generally, if f is a polynomial with integer coefficients, then $f(a) \equiv f(b) \bmod m$. Warning: It is *not* necessarily true that $a^c \equiv b^d \bmod m$.

2. Unique factorization (a.k.a. the Fundamental Theorem of Arithmetic): Every integer can be written uniquely as a product of prime numbers, up to permutations of the prime factors.

3. The Chinese remainder theorem: If m and n are coprime, then the system

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

   has a unique solution mod mn. Ditto for any number of simultaneous congruences, as long as the moduli are *pairwise* coprime.

4. Bézout's identity: If m and n are two integers with gcd d there exist integers a and b such that $am + bn = d$. In other words, m has a multiplicative inverse mod n and vice versa. This also works for polynomials in one variable over fields, which is likewise extremely useful.

5. Fermat's little theorem: If p is a prime number and a is not divisible by p then $a^{p-1} \equiv 1 \pmod p$. More generally, Euler's theorem: if n is an integer, let $\varphi(n) = n \prod_{p|n}(1-1/p)$ where the product is over the prime divisors of n, each prime appearing a single time. Then if a is coprime to n then $a^{\varphi(n)} \equiv 1 \pmod n$.

6. If p is a prime number, then the exponent of p in the prime factorization of $n!$ is $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots$.

Some more advanced facts:

7. The group of units $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic if p is odd, and

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \{\pm 1\} \times \{1, 3, 3^2, \ldots, 3^{2^{n-2}-1}\}.$$

8. You can factor uniquely into primes in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ where ω is a 3rd root of unity.

9. If p is an odd prime, the Legendre symbol $\left(\frac{x}{p}\right)$ is defined as 0 if $p \mid x$, 1 if x is a nonzero square mod p, and -1 otherwise. It has nice properties:

   - Euler's criterion: $\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \bmod p$.
   - Multplicativity: $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
   - $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ and $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$
   - Quadratic reciprocity: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ if p and q are odd primes.

Modular arithmetic

Easier

1. Show that the equation $x^2 + x + 1 = 11y$ has no integer solutions. [Hint: What can the left hand side be mod 11?]

2. (Putnam 1977) Show that $\binom{pa}{pb} \equiv \binom{a}{b} \pmod p$ for all $a \geq b \geq 0$ integers and primes p.

3. Suppose p is a prime $\equiv 3 \pmod 4$. If $p \mid x^2 + y^2$ then $p \mid x$ and $p \mid y$. [Hint: If not, then -1 would be a square mod p.]

Harder

4. Show that there exist no primes p such that for some multiple m of p one has $\binom{m+p}{p} \equiv 1 \pmod m$. (AMM 12030)

5. (Putnam 1985) Let $a_1 = 3$ and for $n \geq 1$ defined $a_{n+1} = 3^{a_n}$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_n? [Hint: If a is coprime to n then $a^b \bmod n = a^{b \bmod \varphi(n)} \bmod n$.]

6. (Putnam 1991) Let p be an odd prime. Show that

$$\sum_{j=0}^{p} \binom{p}{j}\binom{p+j}{j} \equiv 1 + 2^p \pmod{p^2}.$$

[Hint: $\binom{p+j}{j}$ is the coefficient of x^p in $(1+x)^{p+j}$.]

Divisibility and equations

Easier

7. (Putnam 1983) How many positive integers n are there such that n is a divisor of either 10^{40} or 20^{30}?

8. (Putnam 1984) For an integer n define $f(n) = 1! + 2! + \cdots + n!$. Find polynomials $P(n)$ and $Q(n)$ such that $f(n+2) = P(n)f(n+1) + Q(n)f(n)$ for all $n \geq 1$.

9. (Putnam 1981) Let $E(n)$ be the largest integer k such that 5^k divides $1^1 \cdot 2^2 \cdot 3^3 \cdots n^n$. Compute $\displaystyle\lim_{n\to\infty} \frac{E(n)}{n^2}$.

Harder

10. Solve in the integers $2^x \cdot 3^y = 1 + 5^z$. [Hint: Mod 4 and mod 9.]

11. (This one is very nice and related to a problem from the handout on polynomials) Let $P(X), Q(X) \in \mathbb{Z}[X]$ be two polynomials of degrees m and n, such that every coefficient of $P(X)$ or $Q(X)$ is either 1 or 2017. If $P(X) \mid Q(X)$, show that $m+1 \mid n+1$. [Hint: mod 3.]

12. (Putnam 1984) For an integer k let $d(k)$ be the number of 1's in the binary expansion of k. Compute in closed form the sum

$$\sum_{k=0}^{2^m-1} (-1)^{d(k)} k^m.$$

[Hint: Expand and differentiate $(1-x)(1-x^2)(1-x^4)\cdots(1-x^{2^{m-1}})$.]

Extra problems

Easier

13. This is an arch-problem, useful for the other ones.

    (a) What kinds of residues do squares have mod 3?
    (b) What kinds of residues do squares have mod 5?
    (c) What kinds of residues do squares have mod 11?
    (d) What kinds of residues do cubes have mod 9?

14. Show that 2002^{2002} cannot be written as a sum of three cubes. [Hint: mod 9.]

15. Consider the sequence (a_n) defined recursively by $a_1 = 2$, $a_2 = 5$, and $a_{n+1} = (2 - n^2)a_n + (2 + n^2)a_{n-1}$ for $n \geq 2$. Do there exist indices p, q, r such that $a_p a_q = a_r$? [Hint: mod 3.]

16. Consider two integers $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 3$. Show that a has a prime divisor $\equiv 3 \pmod 4$ and b has a prime divisor $\equiv 2 \pmod 3$.

17. Let p be an odd prime. Expand $(x - y)^{p-1}$ reducing the coefficients mod p.

18. Pythagorean triples. Show that the only solutions to $x^2 + y^2 = z^2$ in the integers are of the form $x = d(m^2 - n^2)$, $y = 2dmn$ and $z = d(m^2 + n^2)$ (up to signs and swapping x with y).

19. Consider the sequence (a_n) defined by $a_0 = A \in \mathbb{Z}_{\geq 1}$ and $a_{n+1} = 2a_n - k^2$ where k^2 is the largest perfect square $\leq a_n$. Show that the sequence (a_n) becomes stationary if and only if A is a perfect square. [Hint: If a_n is not a perfect square then it has to be between two consecutive perfect squares. Deduce that the same is true of a_{n+1}.]

20. Find all integers n such that $\dfrac{n^3 - 3n^2 + 4}{2n - 1}$ is an integer.

21. Show that in the product $1! \cdot 2! \cdot 3! \cdots 99! \cdot 100!$ one factor can be removed to get a perfect square.

22. Show that $2^n \nmid n!$ for any $n \geq 1$.

Harder

23. Use the Problems 16 and 13 to find all integers n such that $2^n - 1 \mid a^2 + 1$ for some integer a. (A harder version replaces $a^2 + 1$ with $a^2 + 9$.)

24. Is it possible to place 2015 positive integers on a circle such that for every pair of adjacent numbers the ratio of the larger one to the smaller one is a prime? [Hint: It's important that 2015 is odd.]

25. As an application of Problem 13 show that the system of equations

$$\begin{cases} 5x^2 + y^2 = z^2 \\ x^2 + 5y^2 = t^2 \end{cases}$$

has no integer solutions. [Hint: Add them up.]

26. (Putnam 1999) Let $\mathcal{S}$ be a finite set of integers, each > 1. Suppose that for each integer n there is some $s \in \mathcal{S}$ such that either $(s, n) = 1$ or $(s, n) = s$. Show that there exist $s, t \in \mathcal{S}$ such that (s, t) is a prime number. [Hint: Seek the smallest positive integer that has common factors with every element of $\mathcal{S}$.]