MATH 13150: Freshman Seminar
Unit 14

1. Powers in mod p arithmetic

In this Unit, we will study powers $a^n \pmod p$. It will turn out that these are much easier to compute then one would imagine.

Let's recall a fable which illustrates how quickly powers can grow.

A merchant in a kingdom long ago did something to benefit the Emperor of the kingdom. The Emperor asked the merchant what he could do to thank the merchant. The merchant asked him to give him a chessboard with one grain of rice on the first square, two grains of rice on the second square, four grains of rice on the third square, eight grains of rice on the fourth square, and so on, so on each successive square, the merchant receives double the amount of rice (a chessboard has 64 squares). The Emperor thinks this is a very small amount, and indeed on the 8th square, the merchant receives only $2^7 = 128$ grains of rice, which is about a tablespoon worth. However, by the end of the second row, the merchant received 2^{15} grains of rice, which is about a gallon, and by the end of the 6th row, the amount of rice was 2^{47} grains, which was more rice than could be found in the kingdom. The emperor realized the merchant had played a trick on him, and had him beheaded, and kept the rice.

This fable has two morals:

(1) If you're going to make fun of someone with power over you, make sure they have a sense of humor.

(2) Powers of 2 get to be really big.

The second moral is important for us.

For example, 2^{60} has 19 digits (or is about one billion billion). 2^{100} has 30 digits or so, which is too big to have a name.

1.1. **Calculating powers.**

Although 2^{60} is a large number, a marvelous fact about modular arithmetic is that we can frequently compute $2^{60} \pmod m$ quite easily.

Let's look at some examples.

EXAMPLE: Compute $2^{60} \pmod{31}$.

To do this, notice that $2^5 \equiv 32 \equiv 1 \pmod{31}$. One of the basic properties of exponents is that

$(a^m)^n = a^{mn}$ for any numbers a, m, n.

This remains true in modular arithmetic. In particular, $(2^5)^{12} \equiv 2^{60} \pmod{31}$. From this we conclude that

$2^{60} \equiv (2^5)^{12} \equiv 1^{12} \equiv 1 \pmod{31}$, where we used the observation $2^5 \equiv 1 \pmod{31}$ in the second equivalence.

EXAMPLE: Compute $2^{423} \pmod{31}$.

To do this, we can divide 5 into 423, and see that it goes in 84 times with remainder 3, or in other words, $423 = 5 \cdot 84 + 3$. From this, we obtain:

$2^{423} = 2^{5\cdot 84+3} \equiv 2^{5\cdot 84} \cdot 2^3 \equiv (2^5)^{84} \cdot 2^3 \equiv 1^{84} \cdot 2^3 \equiv 1 \cdot 8 \equiv 8 \pmod{31}$.

In conclusion, $2^{423} \equiv 8 \pmod{31}$.
To do this, we only needed to know that $2^5 \equiv 1 \pmod{31}$, and use powers of exponents:
$a^{b \cdot c} \equiv (a^b)^c \pmod{m}$, $a^{b+c} \equiv a^b \cdot a^c \pmod{m}$.
In this Unit, we'll learn a systematic way of finding identities like $2^5 \equiv 1 \pmod{31}$.

Before we get seriously into that issue, let's think for a moment about computing powers in modular arithmetic. The problem with computing powers is that they get to be really big. The nice feature about modular arithmetic is that it gives us a way to rewrite big numbers as small ones. For example, when we say $519 \equiv 9 \pmod{17}$, we're replacing the big number 519 by the small number 9. Let's think about how we can organize calculatiions to make them feasible.

EXAMPLE: Compute $5^{21} \pmod{31}$.

5^{21} has 15 digits, and can't be easily expressed in usual arithmetic. For modular arithmetic, we can do better.
Note that $5^2 \equiv 25 \pmod{31}$. Further, $25 \equiv -6 \pmod{31}$, so $5^2 \equiv -6 \pmod{31}$.
Now $5^4 \equiv (5^2)^2 \equiv (-6)^2 \equiv 36 \equiv 5 \pmod{31}$, so
$5^4 \equiv 5 \pmod{31}$. Similarly,
$5^8 \equiv (5^4)^2 \equiv 5^2 \equiv 25 \equiv -6 \pmod{31}$, so $5^8 \equiv -6 \pmod{31}$. Similarly,
$5^{16} \equiv (-6)^2 \equiv 36 \equiv 5 \pmod{31}$, so $5^{16} \equiv 5 \pmod{31}$.
We could try computing 5^{32}, but 32 is already bigger than 21. Instead, we can express 21 in terms of 16 and smaller numbers:
$21 = 16 + 4 + 1$.
The trick to doing this is to note that $21 - 16 = 5$, so $21 = 16 + 5$. The smallest power of 2 less than 5 is 4, and $5 - 4 = 1$, or $5 = 4 + 1$. 1 is already a power of 2 since $1 = 2^0$. Putting this together, gives
$21 = 16 + 5 = 16 + (4 + 1) = 16 + 4 + 1$.
$5^{21} \equiv 5^{16+4+1} \equiv 5^{16} \cdot 5^4 \cdot 5^1 \equiv 5 \cdot 5 \cdot 5 \equiv 5^2 \cdot 5 \equiv -6 \cdot 5 \equiv -30 \equiv 1 \pmod{31}$. In other words,
$5^{21} \equiv 1 \pmod{31}$.
We can do that with any number, and once you get used to doing this, it is routine and fast.

PROBLEM: Compute $7^{14} \pmod{31}$.
First, compute powers of 7 in mod 31 arithmetic. For some of these steps, using a calculator is a good idea
$7^2 \equiv 49 \equiv 18 \equiv -13 \pmod{31}$.
$7^4 \equiv (7^2)^2 \equiv (-13)^2 \equiv (13)^2 \equiv 169 \equiv 14 \pmod{31}$.
$7^8 \equiv (7^4)^2 \equiv (14)^2 \equiv 196 \equiv 10 \pmod{31}$. We won't compute 7^{16} since 16 is larger than the power 14. Instead, we'll express 14 in terms of the powers we computed:
$14 - 8 = 6$, so $14 = 8 + 6$.
$6 - 4 = 2$, so $6 = 4 + 2$, and
$14 = 8 + 4 + 2$. This means:
$7^{14} \equiv 7^{8+6+2} \equiv 7^8 \cdot 7^4 \cdot 7^2 \equiv 10 \cdot 14 \cdot -13 \equiv -1820 \equiv -22 \equiv 9 \pmod{31}$,
so $7^{14} \equiv 9 \pmod{31}$. This solves the problem.

You won't have to do problems much bigger than this past problem. We can summarize what we've done as follows:

TECHNIQUE FOR COMPUTING $a^n \pmod{m}$:

STEP 1: Compute $a^2 \pmod{m}$, $a^4 \pmod{m}$, $a^8 \pmod{m}$, $a^{16} \pmod{m}$, etc., where we stop computing when the power in the exponent is larger than n.
STEP 2: Express n as a sum of powers of 2.
STEP 3: Compute $a^n \pmod{m}$ using the law of exponents to express a^n as a product of powers of a we have already computed mod m.
These steps summarize what we did in the examples.

1.2. **Tables of powers.** We want to understand how to compute $a^n \pmod{m}$ even when n is very large. For this, it is useful to know that a certain power is 1.
We can compute powers mod 7 fairly easily. For example:
$2^1 \equiv 2 \pmod{7}$
$2^2 \equiv 4 \pmod{7}$
$2^3 \equiv 1 \pmod{7}$
$2^4 \equiv 2 \pmod{7}$
$2^5 \equiv 4 \pmod{7}$
$2^6 \equiv 1 \pmod{7}$
$2^7 \equiv 2 \pmod{7}$,
$\ldots$
You can probably guess that the $2, 4, 1$ pattern will repeat over and over, so $2^8 \equiv 4 \pmod{7}$, $2^9 \equiv 1 \pmod{7}$.
By doing these calculations, we can compute a table of powers mod 7. In this table, the entry in the $n = 2$ column of the 5^n row is 4 because $5^2 \equiv 4 \pmod{7}$. All entries in the 1^n row are 1 because $1^n = 1$ for any number n.

MOD 7 TABLES OF POWERS

n	1	2	3	4	5	6	7	8	9	10	11	12
1^n	1	1	1	1	1	1	1	1	1	1	1	1
2^n	2	4	1	2	4	1	2	4	1	2	4	1
3^n	3	2	6	4	5	1	3	2	6	4	5	1
4^n	4	2	1	4	2	1	4	2	1	4	2	1
5^n	5	4	6	2	3	1	5	4	6	2	3	1
6^n	6	1	6	1	6	1	6	1	6	1	6	1

While this table is a little tedious to work out, it's not so bad. Once we find a 1 in a row, then the pattern repeats. Indeed, once we know $3^6 \equiv 1 \pmod{7}$, then $3^7 \equiv 3^6 \cdot 3^1 \equiv 1 \cdot 3^1 \pmod{7}$, and $3^8 \equiv 3^6 \cdot 3^2 \equiv 1 \cdot 3^2 \pmod{7}$, and so forth, so $3^9 \equiv 3^3 \pmod{7}$, $3^{10} \equiv 3^4 \pmod{7}$ and so on. In other words, in any row, we only need to go far enough to find a 1, and then we know that the pattern repeats for the rest of the row.

The really important observation is that in the 6-column, all entries are 1. This means that

$a^6 \equiv 1 \pmod 7$ unless $a \equiv 0 \pmod 7$.

Let's also look at powers mod 5:

TABLE OF POWERS MOD 5

n	1	2	3	4	5	6	7	8	9	10	11	12
1^n	1	1	1	1	1	1	1	1	1	1	1	1
2^n	2	4	3	1	2	4	3	1	2	4	3	1
3^n	3	4	2	1	3	4	2	1	3	4	2	1
4^n	4	1	4	1	4	1	4	1	4	1	4	1

Note that once a 1 appears in any row, the remaining elements in the row are given by repeating the pattern up to the 1. Also notice that all entries in the 4 column are 1, or in other words, :

$a^4 \equiv 1 \pmod 5$ unless $a \equiv 0 \pmod 5$.

1.3. **Fermat's Theorem.** Notice that 5 and 7 are primes, and:

$a^4 \equiv 1 \pmod 5$ unless $a \equiv 0 \pmod 5$ and:

$a^6 \equiv 1 \pmod 7$ unless $a \equiv 0 \pmod 7$.

You may have noticed that 5 and 7 are prime, and $4 = 5 - 1$ and $6 = 7 - 1$. This suggests the following result:

Theorem 1.1. *(FERMAT)* $a^{p-1} \equiv 1 \pmod p$ *if* p *is prime, unless* $a \equiv 0 \pmod p$.

Let's try this out when $p = 11$. This predicts that:

$1^{10} \equiv 1 \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$

$3^{10} \equiv 1 \pmod{11}$

$4^{10} \equiv 1 \pmod{11}$

$5^{10} \equiv 1 \pmod{11}$

$6^{10} \equiv 1 \pmod{11}$

$7^{10} \equiv 1 \pmod{11}$

$8^{10} \equiv 1 \pmod{11}$

$9^{10} \equiv 1 \pmod{11}$

$10^{10} \equiv 1 \pmod{11}$

Let's try to verify that $3^{10} \equiv 1 \pmod{11}$, which we can do using the following steps:

$3^2 \equiv 9 \equiv -2 \pmod{11}$

$3^4 \equiv (3^2)^2 \equiv (-2)^2 \equiv 4 \pmod{11}$

$3^8 \equiv (3^4)^2 \equiv 4^2 \equiv 5 \pmod{11}$

$3^{10} \equiv 3^8 \cdot 3^2 \equiv 5 \cdot -2 \equiv -10 \equiv 1 \pmod{11}$!!!

From this, we can use the fact that $8 \equiv -3 \pmod{11}$ to deduce that $8^{10} \equiv (-3)^{10} \equiv (-1)^{10} \cdot 3^{10} \equiv 1 \cdot 1 \equiv 1 \pmod{11}$.

Similarly, since $9 \equiv 3^2 \pmod{11}$, $9^{10} \equiv (3^2)^{10} \equiv 3^{20} \equiv (3^{10})^2 \equiv 1^2 \equiv 1 \pmod{11}$. Since also $2 \equiv -9 \pmod{11}$, $2^{10} \equiv (-9)^{10} \equiv (-1)^{10} \cdot 9^{10} \equiv 1 \cdot 1 \equiv 1 \pmod{11}$. Continuing in this vein, we can verify that each of the above powers is really 1 (mod 11).

I'm willing to bet that you believed me once I wrote down the theorem, so while this kind of exercise has a certain charm, it's not essential.

The following problems illustrate Fermat's theorem.

PROBLEM: Compute $13^{30} \pmod{31}$.

This is really easy to do using Fermat's theorem. Since 31 is prime and 31 does not divide 13, Fermat's theorem asserts that
$13^{30} \equiv 1 \pmod{31}$.
No work required!!!

PROBLEM: Compute the following powers in modular arithmetic:
$17^{42} \pmod{43}$
$121^{58} \pmod{59}$
$142^{210} \pmod{211}$
$21^6 \pmod{7}$

The first three are straightforward:
43 is prime and doesn't divide 17 evenly, so $17^{42} \equiv 1 \pmod{43}$
59 is prime and doesn't divide 121 evenly, so $121^{59} \equiv 1 \pmod{59}$
211 is prime and doesn't divide 142 evenly, so $142^{210} \equiv 1 \pmod{211}$.
The last one has a bit of a twist:
Since 7 divides 21 evenly, $21 \equiv 0 \pmod{7}$, so $21^6 \equiv 0^6 \equiv 0 \pmod{7}$.
In conclusion, the answer to the first three problems is 1 and the answer to the last problem is 0.

Fermat's theorem has some powerful consequences. Let's look at a few of them before moving on.

PROBLEM: Compute $3^{481} \pmod{19}$.

To solve this, note that by Fermat's theorem, $3^{18} \equiv 1 \pmod{19}$. To compute 3^{481}, we divide 18 into 481 using a calculator. Since 18 divides 481 26 times with remainder 13, this means that
$481 = 26 \cdot 18 + 13$. From this, we can deduce that:
$3^{481} \equiv 3^{18 \cdot 26 + 13} \equiv (3^{18})^{26} \cdot 3^{13} \pmod{19}$.
Since $3^{18} \equiv 1 \pmod{19}$, we can write this last expression as:
$3^{481} \equiv 1^{26} \cdot 3^{13} \equiv 3^{13} \pmod{19}$. Now we compute $3^{13} \pmod{19}$ using the method of Section 1.1. We get:
$3^2 \equiv 9 \pmod{19}$
$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv 5 \pmod{19}$
$3^8 \equiv (3^4)^2 \equiv 5^2 \equiv 25 \equiv 6 \pmod{19}$.
Since $13 = 8 + 4 + 1$, $3^{13} \equiv 3^8 \cdot 3^4 \cdot 3^1 \equiv 6 \cdot 5 \cdot 3 \equiv 14 \pmod{19}$. In conclusion,
$3^{481} \equiv 3^{13} \equiv 14 \pmod{19}$.

PROBLEM: Compute $7^{465} \pmod{23}$.

Using Fermat's theorem, $7^{22} \equiv 1 \pmod{23}$. Now divide 22 into 465 to get $465 = 22 \cdot 21 + 3$. This tells us that
$7^{465} \equiv (7^{22})^{21} \cdot 7^3 \equiv 1^{21} \cdot 7^3 \equiv 7^3 \pmod{23}$.
Since $7^2 \equiv 49 \equiv 3 \pmod{23}$, $7^3 \equiv 7^2 \cdot 7 \equiv 3 \cdot 7 \equiv 21 \pmod{23}$, so:
$7^{465} \equiv 21 \pmod{23}$.

REMARK: If $a^{p-1} \equiv 1 \pmod{p}$, and $p-1$ divides n with remainder r, then $a^n \equiv a^r \pmod{p}$.

For example, the remark says that since 22 divides 465 with remainder 3, $7^{465} \equiv 7^3 \pmod{23}$.

PROBLEM: Compute $3^{974} \pmod{11}$.

By Fermat's theorem, $3^{10} \equiv 1 \pmod{11}$. It is easy to see that 10 divides 974 with remainder 4, so if we use the last remark, we see that:
$3^{974} \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}$.

PROBLEM: Compute $5^{579} \pmod{29}$.

To solve this, use Fermat's theorem to conclude that $5^{28} \equiv 1 \pmod{29}$. Now check that 28 divides 579 with remainder 19, so using the above remark,
$5^{579} \equiv 5^{19} \pmod{29}$.
To compute $5^{19} \pmod{29}$, use the following steps:
$5^2 \equiv 25 \equiv -4 \pmod{29}$.
$5^4 \equiv (5^2)^2 \equiv (-4)^2 \equiv 16 \pmod{29}$.
$5^8 \equiv (5^4)^2 \equiv (16)^2 \equiv 256 \equiv 24 \equiv -5 \pmod{29}$.
$5^{16} \equiv (5^8)^2 \equiv (-5)^2 \equiv 25 \equiv -4 \pmod{29}$.
Since $19 = 16 + 2 + 1$,
$5^{19} \equiv 5^{16} \cdot 5^2 \equiv 5^1 \equiv -4 \cdot -4 \cdot 5 \equiv 22 \pmod{29}$, so
$5^{579} \equiv 22 \pmod{29}$.

1.4. **Justification of Fermat's theorem.** Let's see how we can justify Fermat's theorem in an example. We'll show that $5^6 \equiv 1 \pmod{7}$ without actually computing any powers. The same argument works in general.
First, let's consider the number $c \equiv 6! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}$. Let's compute the 5-row of the multiplication table mod 7:
$5 \cdot 1 \equiv 5 \pmod{7}$
$5 \cdot 2 \equiv 3 \pmod{7}$
$5 \cdot 3 \equiv 1 \pmod{7}$
$5 \cdot 5 \equiv 4 \pmod{7}$
$5 \cdot 6 \equiv 2 \pmod{7}$.
It follows that:
(EQUATION *) $5 \cdot 1 \cdot 5 \cdot 2 \cdot 5 \cdot 3 \cdot 5 \cdot 4 \cdot 5 \cdot 5 \cdot 5 \cdot 6 \equiv 5 \cdot 3 \cdot 1 \cdot 6 \cdot 4 \cdot 2 \pmod{7}$.
The left-hand side of this last equality can be written as:
$5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 5^6 \cdot 6!$.
The right-hand side of EQUATION (*) can be written as $5 \cdot 3 \cdot 1 \cdot 6 \cdot 4 \cdot 2 \equiv 6! \pmod{7}$.
If we plug these two equalities back into EQUATION (*), we get:
$5^6 \cdot 6! \equiv 6! \pmod{7}$.

But $\gcd(6!, 7) = 1$, so we can divide by 6! in mod 7 arithmetic, so we find:
$5^6 \cdot \frac{6!}{6!} \equiv \frac{6!}{6!} \pmod 7$.
Since $\frac{6!}{6!} \equiv 1 \pmod 7$, this gives us:
$5^6 \equiv 1 \pmod 7$. That's the end of the argument.
To show that $a^{p-1} \equiv 1 \pmod p$ when p does not divide a, we need to know that the a-row of multiplication mod p contains every element exactly once. In other words, $a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot p - 1$ is the same collection of mod p numbers as 1, 2, 3, ..., p-1. This tells us that
$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot \cdots \cdot a \cdot p - 1 \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot p - 1$,
because the factors on each side of the $\equiv$ sign are the same, but in different orders. We rewrite the lefthand side as: $a^{p-1} \cdot (p-1)!$ and rewrite the righthand side as $(p-1)!$. This tells us that:
$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p$, so dividing each side by $(p-1)!$, we get $a^{p-1} \equiv 1 \pmod p$, just as Fermat's theorem asserts.

EXERCISES:

(1) Compute $7^{13} \pmod{23}$ and $7^{19} \pmod{23}$.
(2) Compute $11^9 \pmod{19}$ and $11^{14} \pmod{19}$.
(3) Compute $2^2 \pmod{13}, 2^3 \pmod{13}, 2^4 \pmod{13}, \ldots, 2^{11} \pmod{13}, 2^{12} \pmod{13}$.
(4) Compute the following powers in modular arithmetic using Fermat's theorem:
  (a) $5^{72} \pmod{73}$
  (b) $11^{78} \pmod{79}$
  (c) $17^{30} \pmod{31}$
  (d) $113^{36} \pmod{37}$
  (e) $15^9 \pmod 3$
  (f) $46^{22} \pmod{23}$
(5) Compute $5^{437} \pmod 3$
(6) Compute $7^{190} \pmod{17}$
(7) Compute $8^{253} \pmod{11}$
(8) Compute $27^{480} \pmod{13}$
(9) In this problem, you are asked to follow the steps explained in the last section of this Unit to explain why $3^{10} \equiv 1 \pmod{11}$.
  (a) Show that $3{\cdot}1 \pmod{11}, 3{\cdot}2 \pmod{11}, 3{\cdot}3 \pmod{11}, \ldots, 3{\cdot}10 \pmod{11}$ are the same as $1 \pmod{11}, 2 \pmod{11}, 3 \pmod{11}, \ldots, 10 \pmod{11}$, but in a scrambled order.
  (b) Show that $3 \cdot 1 \cdot 3 \cdot 2 \cdot 3 \cdot 3 \cdots 3 \cdot 10 \equiv 1 \cdot 2 \cdot 3 \cdots 10 \pmod{11}$ using Part (a).
  (c) Use Part (b) to show that $3^{10} \cdot 10! \equiv 10! \pmod{11}$.
  (d) Use Part (c) to explain the proof that $3^{10} \equiv 1 \pmod{11}$.