Fast Exponentiaion Mod n
Exposition by William Gasarch

1 How to Computer $3^{1000} \pmod{987}$

Lets say you want to compute $3^{1000} \pmod{987}$. There are three ways to do it: idiotic, naive, and smart

Idiotic: Compute 3^{1000}. This will be really big! Then divide it by 987 and find the remainder. This takes 1000 steps and space of roughly 1000 digits.

Naive: Compute $3 \times 3 \times 3 \cdot$ BUT whenever the partial product is over 987, mod it down. This still takes 1000 steps but far less space- about 4 digits.

Smart: Computer

$a_0 = 3 \pmod{987}$ NOTE: $a_0 = 3^{2^0}$.
$a_1 = a_0^2 \pmod{987}$ NOTE: $a_1 = 3^{2^1} \pmod{987}$.
$a_2 = a_1^2 \pmod{987}$ NOTE: $a_2 = 3^{2^2} \pmod{987}$.
$a_3 = a_2^2 \pmod{987}$ NOTE: $a_3 = 3^{2^3} \pmod{987}$.
$a_4 = a_3^2 \pmod{987}$ NOTE: $a_4 = 3^{2^4} \pmod{987}$.
$a_5 = a_4^2 \pmod{987}$ NOTE: $a_5 = 3^{2^5} \pmod{987}$.
$a_6 = a_5^2 \pmod{987}$ NOTE: $a_6 = 3^{2^6} \pmod{987}$.
$a_7 = a_6^2 \pmod{987}$ NOTE: $a_7 = 3^{2^7} \pmod{987}$.
$a_8 = a_7^2 \pmod{987}$ NOTE: $a_8 = 3^{2^8} \pmod{987}$.
$a_9 = a_8^2 \pmod{987}$ NOTE: $a_9 = 3^{2^9} \pmod{987}$.

I stop here since $2^9 \leq 987 < 2^{10}$.

Write 987 in base 2. We'll actually do this:

The highest power of 2 that is ≤ 987 is 512. Hence we subtract this to obtain
$987 = 512 + 475$
The highest power of 2 that is ≤ 475 is 256. Hence we subtract this to obtain
$987 = 512 + 256 + 219$
The highest power of 2 that is ≤ 219 is 128. Hence we subtract this to obtain
$987 = 512 + 256 + 128 + 91$
The highest power of 2 that is ≤ 91 is 64. Hence we subtract this to obtain
$987 = 512 + 256 + 128 + 64 + 27$
The highest power of 2 that is ≤ 27 is 16. Hence we subtract this to obtain
$987 = 512 + 256 + 128 + 64 + 16 + 11$
The highest power of 2 that is ≤ 11 is 8. Hence we subtract this to obtain
$987 = 512 + 256 + 128 + 64 + 16 + 8 + 3$
The highest power of 2 that is ≤ 3 is 2. Hence we subtract this to obtain
$987 = 512 + 256 + 128 + 64 + 16 + 8 + 2 + 1 = 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^1 + 2^0$

AH- we have written 987 as a sum of powers of two. Now we get

$3^{987} \pmod{987} \equiv a_9 \times a_8 \times a_7 \times a_6 \times a_4 \times a_3 \times a_2 \times a_1 \times a_0 \pmod{987}$

More geneally, the idiotic and naive methods to computer $a^n \pmod m$ takes roughly n steps, wheras the method above, called *repeated squaring* takes roughly $\log n$ steps.

2 How to Compute $a^{100000000000000000} \pmod n$

What if the exponent is *really really large*. Then we will apply a technique before using repeated squaring. This requires some math.

Lemma 2.1 *If $n = \frac{x}{y}$ is an integer and p is a prime that divides x but not y then p divides n.*

Proof: Factor both x and y. There will be a factor of p in x but not in y. When you reduce to lowest terms all of the prime factors of y will go away. Some of the prime factors of x will go away, but not p. Hence p will remain. This yields a factorization of x where p is one of the factors. ∎

The following lemma you should know from when you studied combinatorics.

Lemma 2.2 *The number of ways to choose b items from a items is $\binom{a}{b} = \frac{a!}{b!(a-b)!}$.*

Lemma 2.3 *For all primes p, for all $1 \leq y \leq p-1$ p divides $\binom{p}{y}$.*

Proof: $\binom{p}{y} = \frac{p!}{y!(p-y)!}$ is an integer where p divides the numerator but not the denominator. By Lemma 2.1 p divides $\binom{p}{y}$. ∎

The following you have surely seen. I may prove it in class

Lemma 2.4 *Let $n \in \mathsf{N}$. Then $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$.*

NOTE- WE HAVE NOT COVERED INDUCTION YET SO JUST TAKE THIS LEMMA AS TRUE. WE"LL RETURN TO THE PROOF LATER IN THE COURSE.

Lemma 2.5 *Let p be a prime and $n \in \mathsf{N}$. Then $n^p \equiv n \pmod p$.*

Proof: We prove this by induction on n.
Base case: If $n = 1$ then $n^p = 1^p = n \pmod p$.
Induction Hypothesis: Assume that $n^p \equiv 1 \pmod p$ and that $n + 1 \leq p - 1$.
Induction Step:

$$(n+1)^p \equiv \sum_{i=0}^{p} \binom{p}{i} n^i 1^{p-i} = \sum_{i=0}^{p} \binom{p}{i} n^i = 1 \times n^0 + \sum_{i=1}^{p-1} \binom{p}{i} + 1 \times n^p.$$

By Lemma 2.3 all of the terms in $\sum_{i=1}^{p-1} \binom{p}{i}$ are $\equiv 0 \pmod{p}$. Hence we have

$$(n+1)^p \equiv \sum_{i=0}^{p} \binom{p}{i} n^i 1^{p-i} = 1 + n^p.$$

By the induction hypothesis $n^p \equiv n \pmod{p}$, so we have $(n+1)^p \equiv n+1 \pmod{p}$.

∎

Lemma 2.6 *If $1 \leq n \leq p-1$ and p is prime then $n^{p-1} \equiv 1 \pmod{p}$.*

Proof: By Lemma 2.5 $n^p \equiv n \pmod{p}$. Hence there is a k such that

$$n^p = n + kp.$$

Divide by n to obtain

$$n^{p-1} = 1 + \frac{kp}{n}.$$

Since $\frac{kp}{n} = n^{p-1} - 1$, $\frac{kp}{n}$ is an integer. Since $n \leq p-1$, p does not divide the denominator n, though p clearly divides the numerator kp. Hence we can apply Lemma 2.1 and conclude that p divides $\frac{kp}{n}$. Hence

$$n^{p-1} \equiv 1 \pmod{p}.$$

∎

Lemma 2.7 *Let p be a prime. Then $a^n \equiv a^{n \pmod{p-1}} \pmod{p}$.*

Proof:

Let $n \equiv n' \pmod{p-1}$ where $0 \leq n' \leq p-1$. Hence $n = n' + k(p-1)$ for some k. Then

$$a^n = a^{n'+k(p-1)} = a^{n'} \times a^{k(p-1)} = a^{n'} \times (a^{p-1})^k$$

By Lemma 2.6 $a^{p-1} \equiv 1 \pmod{p}$. Hence we have $a^n \equiv a^{n'} \pmod{p}$. ∎

So, how can we use this? Let p be a prime. Then

$$a^n \pmod{p} = a^{n \pmod{p-1}} \pmod{p}.$$

Hence if n is ginormous then we first mod it by $p-1$ so it will be $\leq p-1$. We will then use repeated squaring.