Notes on Modular Exponentiation and Euler Function (WITH ASSIGNMENT)

Dr. Holmes

April 12, 2007

There are problems to be turned in (all starred) at the end of this document.

1 Modular Exponentiation

Basic Fact: $a^x \equiv (a \bmod n)^x \bmod n$ (you can replace the base in an exponentiation by its remainder mod n if you are working in mod n arithmetic). But a^x is not necessarily congruent to $a^{x \bmod n}$ modulo n: for example, 3 is equivalent to 13 in mod 10 arithmetic, but $7^3 = 343$ is not equivalent to $7^{13} = 96889010407$: the first is equivalent to 3 mod 10 while the second is equivalent to 7.

Repeated Squaring: A technique which allows efficient computation of powers in modular arithmetic (though not nearly as efficient as the method using Euler's function below) is the method of repeated squaring.

To compute $a^x \bmod n$, note that the exponent x is either even or odd. If $x = 2k$ is even, then $a^x = a^{2k} = (a^k)^2$: compute a^k then square it. If $x = 2k + 1$ is odd, then $a^x = a^{2k+1} = a^{2k} \cdot a = (a^k)^2 \cdot a$. Either way, we compute the square of $a^{x \operatorname{div} 2}$ and multiply by $a^{x \bmod 2}$ (the latter being either 1 or a).

We give an example:

Compute 7^{330} mod 13.

The powers of 7 that we need to compute are obtained by dividing 330 by 2 repeatedly (throwing away remainders):

330, 165, 82, 41, 20, 10, 5, 2, 1

$7^1 = 7$ mod 13

$7^2 = 7 \cdot 7 = 49 = 10 \bmod 13$
$7^5 = (7^2)^2 \cdot 7 = 10^2 \cdot 7 = 11 \bmod 13$
$7^{10} = (7^5)^2 = 11^2 = 121 = 4 \bmod 13$
$7^{20} = (7^10)^2 = 4^2 = 16 = 3 \bmod 13$
$7^{41} = (7^{20})^2 \cdot 7 = 3^2 \cdot 7 = 63 = 11 \bmod 13$
$7^{82} = (7^{41})^2 = 11^2 = 121 = 4 \bmod 13$
$7^{165} = (7^{82})^2 \cdot 7 = 4^2 \cdot 7 = 8 \bmod 13$
$7^{330} = (7^{165})^2 = 8^2 = 64 = 12 \bmod 13$
so the answer is 12.

To compute 7^{330} the naive way would take 329 multiplications; in general, a^x would take $x - 1$ multiplications. The method of repeated squaring takes (roughly speaking) 1 or 2 multiplications for each power of two below x: the number of multiplications needed is at most $2 \cdot \lceil \log_2(x) \rceil$. Here we needed 11 multiplications.

2 Euler's Function

For any positive integer n we define $\phi(n)$ as the number of positive integers $a < n$ such that a is relatively prime to n.

First Fact:

$\phi(p) = p - 1$ if p is a prime. In this case, the positive integers less than p which are relatively prime to p are all of them: $1, 2, \ldots, p - 1$ are a total of $p - 1$ positive integers less than p which are relatively prime to p.

Second Fact:

$\phi(p^n) = p^n - p^{n-1}$ for p a prime. There are $p^n - 1$ positive integers less than p^n. Of these, only the multiples of p are not relatively prime to p^n, and there are $p^{n-1} - 1$ of these. So there are $(p^n - 1) - (p^{n-1} - 1) = p^n - p^{n-1}$ positive integers less than p^n which are relatively prime to p^n.

Third Fact:

If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

There are exactly as many natural numbers less than mn as there are systems of equations

$x = a \bmod m$
$x = b \bmod n$

with $0 \leq a < m$ and $0 \leq b < n$, because by the Chinese Remainder Theorem each of these mn equations has a unique solution mod mn.

A solution to one of these equations is relatively prime to mn just in case a is relatively prime to m and b is relatively prime to n. This means that there are $\phi(m)$ possible choices of a and $\phi(n)$ possible choices of b that work, and thus there are $\phi(m)\phi(n)$ positive integers less than mn (0 is not a possible choice) which are relatively prime to mn.

All of this only works if $\texttt{gcd}(m, n) = 1$ (if m and n are relatively prime).

Computing Euler's Function

If we know the prime factorization of n we can compute $\phi(n)$. Because we know how to compute Euler's function for powers of primes, and because the powers of different primes are relatively prime to each other, we can take the values of Euler's function at the prime powers in the factorization of n and multiply these together.

We give examples.

$\phi(5) = 4$. 5 is a prime, so we just subtract 1.

$\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2) \cdot \phi(3) = (2^2 - 2^1) \cdot (3 - 1) = 4$

$\phi(200) = \phi(2^3 \cdot 5^2) = (2^3 - 2^2) \cdot (5^2 - 5^1) = 4 \cdot 20 = 80$

$\phi(90) = \phi(2 \cdot 3^2 \cdot 5) = (2 - 1) \cdot (3^2 - 3^1) \cdot (5 - 1) = 30$

3 Modular Exponentiation using Euler's Function

The big theorem (of which we will probably only prove the special case with n a prime number)

is

$$a^x \equiv a^{x \bmod \phi(n)} \bmod n$$

This follows from the fact that

$$a^{\phi(n)} \equiv 1 \bmod n$$

so $a^x = a^{q\phi(n)+r} = (a^{\phi(n)})^q \cdot a^r = 1^q \cdot a^r = a^r$

where $q = x \,\texttt{div}\, \phi(n)$ and $r = x \bmod \phi(n)$.

We can replace the base of an exponentiation in mod n arithmetic with its remainder on division by n, and we can replace the exponent with its remainder on division by $\phi(n)$. This is much more effective than repeated squaring (though we might also use repeated squaring if $\phi(n)$ is very large).

We also might have to use repeated squaring if we do not know the prime factorization of n, since our ability to compute $\phi(n)$ depends on being able to factor n.

Example of calculation of a power by this method:
Compute $1243542535^{23415675437654} \bmod 18$.
$\phi(18) = \phi(2 \cdot 3^2) = (2-1) \cdot (3^2 - 3^1) = 6$
$1243542535 \,\texttt{mod}\, 18 = 7$
$23415675437654 \,\texttt{mod}\, 6 = 2$
so $1243542535^{23415675437654} = 7^2 = 49 = 13 \bmod 18$.

4 Exercises

1. Compute $7^{1115} \,\texttt{mod}\, 11$ by the method of repeated squaring.

2. Compute the following values of the Euler function:

$$\phi(37), \phi(125), \phi(45), \phi(144), \phi(143), \phi(300)$$

3. Compute $7^{1115} \,\texttt{mod}\, 11$ (same as first problem) using the Euler function to reduce the exponent.

4. Compute $34247^{41467} \,\texttt{mod}\, 33$ by whatever method or combination of methods works.