Lecture 9 - Squares and Roots mod m

In the next lecture we will describe the RSA cryptosystem which is a public-key cryptosystem which allows individuals to securely send messages to one another. Today we'll spend some time discussing two techniques to make the calculations we'll need in RSA more tractable.

Suppose a, k, and m are very large integers having, say, 100 digits each. Is there an effective method for computing a^k modulo m? If k is very large it's extremely difficult — even on a very fast computer to naïvely compute a^k by multiplying a with itself k times. We can compute a^k modulo m if we take advantage of the following trick:

Suppose k appears in binary as

$$k = u_n u_{n-1} u_{n-2} \cdots u_1 u_0$$

where each u_i is zero or one. That is,

$$k = u_n 2^n + u_{n-1} 2^{n-1} + u_{n-2} 2^{n-2} + \cdots + u_1 2 + u_0$$

E.g., 157 in binary is 10011101:

$$157 = 1 \cdot 2^7 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1$$

Now, if $k = u_n 2^n + u_{n-1} 2^{n-1} + \cdots + u_1 2 + u_0$, then

$$a^k = a^{u_0 + u_1 2 + u_2 2^2 + \cdots + u_{n-1} 2^{n-1} + u_n 2^n}$$

$$= a^{u_0} \cdot a^{u_1 2} \cdot a^{u_2 2^2} \cdot \cdots \cdot a^{u_{n-1} 2^{n-1}} \cdot a^{u_n 2^n}$$

$$= a^{u_0} \cdot [a^2]^{u_1} \cdot [a^4]^{u_2} \cdots [a^{2^{n-1}}]^{u_{n-1}} \cdot [a^{2^n}]^{u_n}$$

For example,

$$3^{157} = 3^1 \cdot [3^2]^0 \cdot [3^4]^1 \cdot [3^8]^1 \cdot [3^{16}]^1 \cdot [3^{32}]^0 \cdot [3^{64}]^0 \cdot [3^{128}]^1$$

$$= 3^0 \cdot 3^4 \cdot 3^8 \cdot 3^{16} \cdot 3^{128}$$

Right now this may not seem like a very helpful operation, but notice each of the factors above which may be raised to a 0 or 1 is the square of the previous factor.

$$[3]^1 \cdot [3^2]^0 \cdot [(3^2)^2]^1 \cdot [((3^2)^2)^2]^1 \cdot [(((3^2)^2)^2)^2]^1 \cdots$$

Now, if we're working with congruence classes, then we can just square the last factor modulo m — and this keeps our numbers from getting too huge.

Let's calculate $3^{157} \pmod{42}$ as an example: First we calculate squares mod 42.

$$\begin{aligned}
3 &\equiv 3 \pmod{42} \\
3^2 &\equiv 9 \pmod{42} \\
3^4 &\equiv 9^2 \equiv 39 \pmod{42} \\
3^8 &\equiv 39^2 \equiv 9 \pmod{42} \\
3^{16} &\equiv 9^2 \equiv 39 \pmod{42} \\
3^{32} &\equiv 9 \pmod{42} \\
3^{64} &\equiv 39 \pmod{42} \\
3^{128} &\equiv 9 \pmod{42}
\end{aligned}$$

Hence

$$\begin{aligned}
3^{157} &\equiv 3 \cdot 39 \cdot 9 \cdot 39 \cdot 9 \pmod{42} \\
&\equiv 369603 \pmod{42} \\
&\equiv 3 \pmod{42}
\end{aligned}$$

This sort of computation is reasonably easy to do on a computer, whereas directly computing 3^{157} is not so easy — 3^{157} has 75 digits.

This computational trick is called the "method of successive squaring" and is summarized below.

The Method of Successive Squaring

To compute $a^k \pmod m$:

① Determine the binary expansion of k:

$$k = u_0 + u_1 \cdot 2 + u_2 \cdot 2^2 + u_3 \cdot 2^3 + \cdots + u_{n-1} 2^{n-1} + u_n 2^n$$

② Make a list of the successive squares of a, modulo m

$$\begin{aligned}
a &\pmod m \\
a^2 &\pmod m \\
a^4 = [a^2]^2 &\pmod m \\
a^8 = [a^4]^2 &\pmod m \\
a^{16} = [a^8]^2 &\pmod m \\
&\vdots \\
a^{(2^n)} = [a^{(2^{n-1})}]^2 &\pmod m
\end{aligned}$$

③ Use the above table and binary expansion of k to determine a^k modulo m

$$\begin{aligned}
a^k &= a^{u_0 + u_1 2 + u_2 2^2 + \cdots + u_n 2^n} \\
&= a^{u_0} \cdot [a^2]^{u_1} \cdot [a^4]^{u_2} \cdots [a^{2^n}]^{u_n} \\
&\equiv a^{u_0} \cdot [a^2]^{u_1} \cdots [a^{2^n}]^{u_n} \pmod m
\end{aligned}$$

Now let's consider the opposite problem. Instead of raising a given value to the k^{th} power modulo m, let's calculate k^{th}-roots of m. That is, let's find the values of x such that

$$x^k \equiv b \pmod{m}$$

To make things easier, let's first suppose

$$\gcd(b,m) = 1$$
$$\gcd(k, \varphi(m)) = 1$$

Hence we can find integers u and v satisfying

$$ku - \varphi(m)v = 1$$

We can in fact find positive integers u and v solving this equation.

Notice this means $ku = 1 + \varphi(m)v$. Hence

$$x^{ku} = x^{1+\varphi(m)v}$$
$$= x \cdot x^{\varphi(m)v}$$

Thus

$$\left(x^k\right)^u \equiv x \left(x^{\varphi(m)}\right)^v \pmod{m}$$

This is true for all values of x, so in particular if $x \equiv b \pmod{m}$ we have

$$b^{ku} \equiv b \cdot (b^{\varphi(m)})^v \pmod{m}$$
$$\Rightarrow (b^u)^k \equiv b \pmod{m}$$

and so b^u (which we can compute by successive squaring) solves $x^k \equiv b \pmod{m}$.

Example

Solve $x^{17} \equiv 11 \pmod{14}$.

By the above we need to solve

$$17u - 6v = 1 \qquad \varphi(14) = \varphi(2 \cdot 7) = 6$$

$u = 11$ and $v = 31$ solve this, and so we claim

$$x = 11^{11} \pmod{14}$$

is a solution to $x^{17} \equiv 11 \pmod{14}$. Note

$$(11^{11})^{17} = 11^{11 \cdot 17} = 11^{1 + 6 \cdot 31}$$
$$= 11 \cdot (11^6)^{31}$$
$$\equiv 11 \pmod{14}.$$