CIS260-201/204–Spring 2008

Modular Exponentiation[1]

Friday, April 25

Let b be a positive integer. The notation a^b means to multiply a by itself repeated, with a total of b factors of a; that is,

$$a^b = \underbrace{a \times a \times \cdots \times a}_{b \text{ times}}.$$

The notation for $\mathbb{Z}_n$ is the same. If $a \in \mathbb{Z}_n$ and b is a positive integer, in the context of $\mathbb{Z}_n$ we define

$$a^b = \underbrace{a \otimes a \otimes \cdots \otimes a}_{b \text{ times}}.$$

This is called modular exponentiation.

Example: Calculate 2^{16} in $\mathbb{Z}_7$.
We see that $2^{16} = 65536$. $65536/7 = 9262.2857...$, so $65536 \text{ div } 7 = 9362$. Now, $9362 \cdot 7 = 65534$, so $65536 \bmod 7 = 65536 - 65534 = 2$. Therefore, $2^{16} = 2$ in $\mathbb{Z}_7$.

That wasn't so bad, especially if we have a calculator. But what if the exponent becomes too large for a calculator to handle? For example, what is 3^{64} in $\mathbb{Z}_{100}$? Then this method of direct exponentiation becomes intractable.

Is there any better way? The answer is yes, and we begin with the following question: Is $a^b = a^{b \bmod n}$? Let's try the above example where $a = 2, b = 16, n = 7$. Then $a^b = 2$, as calculated above. Now, $a^{b \bmod n} = 2^{16 \bmod 7} = 2^2 = 4$. But $2 \neq 4$, so this statement is false.

So merely modulo-ing the exponent does not help. Let's try another way. Instead of directly calculating the exponentiation and mod, why don't we take a power at a time and reduce the remainder as necessary? Moreover, to calculate some power, we don't need to multiply by a repeatedly. Once we have a^b, if we multiply this to itself, we get a^{2b}. If we do that again to a^{2b}, we get a^{4b}. This will take us to the destination much faster. Consider the last example again.

Example: Calculate 2^{16} in $\mathbb{Z}_7$.
We have $2^2 = 4$, so $2^4 = 16$, so now we can reduce the remainder as $16 \equiv 2 \pmod 7$. Doing this again, we obtain

$$\begin{aligned} 2^8 &\equiv 4 \pmod 7 \\ 2^{16} &\equiv 16 \equiv 2 \pmod 7, \end{aligned}$$

as expected.

Let's try a more complicated example mentioned earlier.

Example: Calculate 3^{64} in $\mathbb{Z}_{100}$.
Once again, we use the method of "repeated squaring" and obtain the following result.

$$3 \equiv 3 \pmod{100}$$

[1]Adapted from Exercise 36.14 in the textbook

$$
\begin{aligned}
3^2 &\equiv 9 \pmod{100} \\
3^4 &\equiv 81 \pmod{100} \\
3^8 &\equiv 6561 \equiv 61 \pmod{100} \\
3^{16} &\equiv 3721 \equiv 21 \pmod{100} \\
3^{32} &\equiv 441 \equiv 41 \pmod{100} \\
3^{64} &\equiv 1681 \equiv 81 \pmod{100}.
\end{aligned}
$$

Hence, $3^{64} = 81$ in $\mathbb{Z}_{100}$.

What if the exponent is not a multiple of 2? Well, we proved by induction before that any number can be written as the sum of the powers of 2, so why don't we use it here?

Example: Calculate 4^{13} in $\mathbb{Z}_9$.

$$
\begin{aligned}
4 &\equiv 4 \pmod{100} \\
4^2 &\equiv 16 \equiv 7 \pmod{100} \\
4^4 &\equiv 49 \equiv 4 \pmod{100} \\
4^8 &\equiv 16 \equiv 7 \pmod{100}.
\end{aligned}
$$

Now, $13 = 8 + 4 + 1$, so $4^{13} = 4^8 4^4 4^1$. Thus, $4^{13} \equiv 7 \cdot 4 \cdot 4 = 28 \cdot 4 \equiv 1 \cdot 4 = 4 \pmod{9}$. That is, $4^{13} = 4$ in $\mathbb{Z}_9$.

If n is small enough, there is another method, presented in the following example.

Example: Find the remainder of 2^{2008} when divided by 7.
First, note that $2^3 \equiv 1 \pmod{7}$. Hence, if we raise 2^3 to any power, the remainder must still be 1. Now, $2008 = 3 \cdot 669 + 1$, so $2^{2008} = 2^{3 \cdot 669} 2^1 = \left(2^3\right)^{669} 2 \equiv 1^{669} 2 = 2 \pmod{7}$. That is, $2^{2008} \bmod 7 = 2$.

Exercises:

1. Let $a, b \in \mathbb{Z}$. Prove that in $\mathbb{Z}_n$, $a^b = (a \bmod n)^b$.
2. What is the last digit of 7^{123456}?
3. What is the last two digits of 101^{2551}?
4. Calculate 2^{2547} in $\mathbb{Z}_{11}$. [**Hint**: $2^5 = 32 \equiv 10 \equiv -1 \pmod{11}$.]
5. Calculate 4^{2008} in $\mathbb{Z}_{13}$.
6. Calculate 5^{63} in $\mathbb{Z}_{66}$.
7. Calculate 121^{2009} in $\mathbb{Z}_{260}$.
8. [Extra Credit!] Calculate 1155^{1234} in $\mathbb{Z}_{123}$. [**Hint**: Factor 1155.]