CONGRUENCES

Let a, b, and n be integers. If $n \neq 0$, we say that ***a* is congruent to *b* modulo *n*** if $a - b$ is divisible by n, which is written $a \equiv b \pmod{n}$. For example, $9 \equiv 1 \pmod{4}$ and $-15 \equiv -3 \pmod{6}$, but $21 \not\equiv 3 \pmod{5}$. Congruences (mod n) depend on the remainder that's obtained in the division algorithm when the divisor is n. For example, since $987 = 197 \cdot 5 + 2$, we know that $987 \equiv 2 \pmod{5}$. Of course, it's also true that $987 \equiv 7 \pmod{5}$ and that $987 \equiv -3 \pmod{5}$, etc., but the idea of a congruence (mod n) is that we throw out any multiple of n and keep only what's left over.

The list below gives several important rules that we can use when working with congruences. The first three of these are similar to the corresponding rules for equalities. Unless otherwise stated, all variables stand for integers, with n restricted to be a positive integer.

1. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
2. If $a \equiv b \pmod{n}$, then for any c,

   $a \pm c \equiv b \pm c \pmod{n}$

   $ac \equiv bc \pmod{n}$
3. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

   $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n}$

   $a_1 a_2 \equiv b_1 b_2 \pmod{n}$
4. For any positive integer c, the statement $a \equiv b \pmod{n}$ is equivalent to the congruences $a \equiv b$, $b + n$, $b + 2n$, . . . , $b + (c - 1)n \pmod{cn}$.
5. If $ab \equiv ac \pmod{n}$, then

   $b \equiv c \pmod{n}$ if $\gcd(a, n) = 1$

   $b \equiv c \left(\mod \frac{n}{d}\right)$ if $d = \gcd(a, n) > 1$
6. **Fermat's Little theorem**. If p is a prime and a is an integer, then

   $a^{p-1} \equiv 1 \pmod{p}$, if p does not divide a

   $a^p \equiv a \pmod{p}$, for any integer a

The rules above can be used to reduce a congruence and solve congruence equations. For example, let's figure out the remainder that results when 3^{10} is divided by 7. We could actually compute 3^{10}, divide by 7, and see what the remainder is, but that's quite a bit of work: Congruences will make this task a lot easier. We're asked to find the value of b such that $3^{10} \equiv b \pmod{7}$, with $0 \leq b < 7$.

First, we notice that 3^2 is congruent to 2 (mod 7). Since $3^{10} = (3^2)^5$, we can apply the third equation in rule 3 above and conclude that $3^{10} = (3^2)^5 \equiv 2^5 \pmod{7}$. Now it's easy to figure out that $2^5 = 32 \equiv 4 \pmod{7}$. Because $3^{10} \equiv 4 \pmod{7}$, the remainder when 3^{10} is divided by 7 is 4.

Example 6.4 What's the remainder when 2^{345} is divided by 29?

Solution: Since 29 is a prime, Fermat's little theorem tells us that $2^{28} \equiv 1 \pmod{29}$.
Since $2^{345} = (2^{28})^{12} \cdot 2^9$, we can conclude that $2^{345} = (2^{28})^{12} \cdot 2^9 \equiv 1^{12} \cdot 2^9 \equiv 2^9 \pmod{29}$.
Now, since $2^5 \equiv 3 \pmod{29}$, we have $2^9 = 2^5 \cdot 2^4 \equiv 3 \cdot 2^4 = 48 \equiv 19 \pmod{29}$.
Therefore, when 2^{345} is divided by 29, the remainder will be 19.