Advertisement. Cryptography is offered in the coming Spring semester.

13 Euler's theorem

Theorem 101. (Euler's theorem) If $n \geqslant 1$ and $\gcd(a,n)=1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. next time

Note that Fermat's little theorem is the special case of prime n:

Fermat's little theorem. If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example 102. What are the last two (decimal) digits of 3^{4242}?

Solution. We need to determine $3^{4242} \pmod{100}$. $\phi(100) = \phi(2^2) \cdot \phi(5^2) = (4-2)(25-5) = 40$.

Since $\gcd(3,100)=1$ and $4242 \equiv 2 \pmod{40}$, Euler's theorem shows that $3^{4242} \equiv 3^2 = 9 \pmod{100}$.

Example 103. Compute $7^{100} \pmod{60}$.

Solution. $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$. Since $\gcd(7,60)=1$, we obtain that $7^{16} \equiv 1 \pmod{60}$ by Euler's theorem. Since $100 \equiv 4 \pmod{16}$, we have $7^{100} \equiv 7^4 \pmod{60}$.

It remains to notice that $7^2 = 49 \equiv -11$ and hence $7^4 \equiv (-11)^2 = 121 \equiv 1 \pmod{60}$. So, $7^{100} \equiv 1 \pmod{60}$.

Comment. See the next example, which shows that we actually have $a^4 \equiv 1 \pmod{60}$ for all integers a coprime to 60.

Example 104. Euler's theorem doesn't necessarily provide an optimal exponent. For instance, show that $a^4 \equiv 1 \pmod{60}$ for all integers a coprime to 60.

Note. Since $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$, Euler's theorem shows that $a^{16} \equiv 1 \pmod{60}$.

Proof. By the Chinese remainder theorem, $a^4 \equiv 1 \pmod{60}$ is equivalent to

$$a^4 \equiv 1 \pmod{4}, \quad a^4 \equiv 1 \pmod{3}, \quad a^4 \equiv 1 \pmod{5}.$$

All three of these congruences are true:

- $a^4 \equiv 1 \pmod{5}$ is true by Fermat's little theorem.
- $a^4 \equiv 1 \pmod{3}$ is true, because $a^2 \equiv 1 \pmod{3}$ by Fermat's little theorem.
- $a^4 \equiv 1 \pmod{4}$ is true, because $a^2 \equiv 1 \pmod{4}$ by Euler's theorem ($\phi(4)=2$).

(Note that a is coprime to 60 if and only if a is coprime to each of 4, 3, 5.) □

Example 105. As in the previous example, show that $a^6 \equiv 1 \pmod{42}$ for all integers a coprime to 42.

Note. Since $\phi(42) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12$, Euler's theorem shows that $a^{12} \equiv 1 \pmod{42}$.

Proof. By the Chinese remainder theorem, $a^6 \equiv 1 \pmod{42}$ is equivalent to

$$a^6 \equiv 1 \pmod{2}, \quad a^6 \equiv 1 \pmod{3}, \quad a^6 \equiv 1 \pmod{7}.$$

But these congruences all follow from Fermat's little theorem (because 6 is a multiple of $2-1=1$, $3-1=2$ and $7-1=6$)! (Note that a is coprime to 42 if and only if a is coprime to each of 2, 3, 7.) □

Advanced. Based on these ideas, can you formulate a general strengthening of Euler's theorem?

https://en.wikipedia.org/wiki/Carmichael_function

Armin Straub
straub@southalabama.edu