Mc Graw Hill Education

Number Theory

Chapter 4

Edited by: Dr. Meshal Alfarhood

Solving Congruences

Section 4.4

Section Summary

Linear Congruences

Finding Inverses

The Chinese Remainder Theorem

Fermat’s Little Theorem

The Euler’s Generalization

Fermat's Little Theorem

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

Examples:

1. $6^{10} \equiv 1 \pmod{11}$ → because p=11 is prime, and $11 \nmid 6$
2. $7^{10} \equiv 1 \pmod{11}$ → because p=11 is prime, and $11 \nmid 7$

Exercise:

Find 7^{222} **mod** 11?

- $7^{10} \equiv 1 \pmod{11}$ from Fermat's Little Theorem.
- $(7^{10})^{22} \equiv (1)^{22} \pmod{11}$ $(7^{10})^k \equiv (1)^k \pmod{11}$
- $7^{220} \equiv 1 \pmod{11}$
- $7^{220} \cdot 7^2 \equiv 1 \cdot 7^2 \pmod{11}$ because $7^{222} = 7^{10\cdot 22+2}$
- 7^{222} **mod** 11 = 7^2 mod 11 = **5**.
- Hence, 7^{222} **mod** 11 = **5**.

$\boxed{7^{222} \equiv 5 \pmod{11}}$

Fermat's Little Theorem$_2$

Exercise: Find 15^{100} **mod** 31?

- $15^{30} \equiv 1 \pmod{31}$ from Fermat's Little Theorem.
- $(15^{30})^3 \equiv (1)^3 \pmod{31}$
- $15^{90} \equiv 1 \pmod{31}$
- $15^{90} \cdot 15^{10} \equiv 1 \cdot 15^{10} \pmod{31}$ because $15^{100} = 15^{30 \cdot 3 + 10}$
- $15^{100} \bmod 31 = 15^{10} \bmod 31$.
- 15^{10} is still a big number:
  - $15 \equiv 15 \pmod{31}$ any number is always congruent to itself
  - $15^2 \equiv 225 \equiv 8 \pmod{31}$
  - $15^4 \equiv 8^2 \equiv 2 \pmod{31}$
  - $15^8 \equiv 2^2 \equiv 4 \pmod{31}$
  - $15^8 \cdot 15^2 \equiv 4 \cdot 15^2 \pmod{31}$
  - $15^{10} \equiv 4 \cdot 8 \pmod{31}$
  - $15^{10} \equiv 32 \equiv 1 \pmod{31}$
  - Hence, 15^{100} **mod** 31 = **1**

$$\boxed{15^{100} \equiv 1 \pmod{31}}$$

The Euler's Generalization

Euler's Totient function Φ(n): the count of numbers < n that are relatively prime to n.

- **Examples:**
  1. **Φ(2) = 1;** |{1}|
  2. **Φ(3) = 2;** |{1,2}|
  3. **Φ(12) = 4;** |{1,5,7,11}|
  4. **Φ(15) = 8;** |{1,2,4,7,8,11,13,14}|
- **Note:** if n is a prime number, then Φ(n) = n-1
- **Φ(n) can also be calculated using the following formula:**
  - $\Phi(n) = n \prod \frac{p-1}{p}$ where p is prime < n, and p|n.
  - **Examples:**
    1. $\Phi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$; $12 = 2^2 \cdot 3$
    2. $\Phi(15) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$; $15 = 3 \cdot 5$

The Euler's Generalization 2

If ***a*** and ***n*** are relatively prime, then $a^{\Phi(n)} \equiv 1 \pmod{n}$.

- **Note:** if n is a prime number, then $\Phi(n) = n-1$
- Therefore, let *n=p,* that leads to Fermat's theorem: $a^{p-1} \equiv 1 \pmod{p}$.
- **Example:** What is the last two digits of 27^{1203}?
  - The last two digits = 27^{1203} **mod** 100
  - Can't use Fermat's because 100 is not prime.
  - Using Euler: $\Phi(100)=40$.
  - $27^{40} \equiv \mathbf{1} \pmod{100}$
  - $(27^{40})^{30} \cdot 27^3 \equiv \mathbf{1^{30}} \cdot 27^3 \pmod{100}$ because $27^{1203} = 27^{40 \cdot 30+3}$
  - 27^{1203} **mod** 100 = 27^3 **mod** 100 = **83**