Lecture 6: Congruences, Part II

William Stein

Math 124 Harvard University **Fall 2001**

Key Ideas Today

- Wilson's theorem
- Chinese Remainder Theorem
- Multiplicativity of φ

1 Wilson's Theorem

Theorem 1.1 (John Wilson's theorem, from the 1770s). *An integer $p > 1$ is prime if and only if*

$$(p-1)! \equiv -1 \pmod{p}.$$

Example 1.2.

```
? p=3
%1 = 3
? (p-1)! % 3
%2 = 2
? p=17
%3 = 17
? (p-1)!
%4 = 20922789888000
? (p-1)! % p
%5 = 16
```

Proof. We first **assume that p is prime** and prove that $(p-1)! \equiv -1 \pmod{p}$. If $a \in \{1, 2, \ldots, p-1\}$ then the equation

$$ax \equiv 1 \pmod{p}$$

has a unique solution $a' \in \{1, 2, \ldots, p-1\}$. If $a = a'$, then $a^2 \equiv 1 \pmod{p}$, so $p \mid a^2 - 1 = (a-1)(a+1)$, so $p \mid (a-1)$ or $p \mid (a+1)$, so $a \in \{1, -1\}$. We can thus pair off the elements of $\{2, 3, \ldots, p-2\}$, each with its inverse. Thus

$$2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}.$$

Multiplying both sides by $p-1$ proves that $(p-1)! \equiv -1 \pmod{p}$.

Next we **assume that** $(p-1)! \equiv -1 \pmod{p}$ and prove that p must be prime. Suppose not, so that p is a composite number ≥ 4. Let ℓ be a prime divisor of p. Then $\ell < p$, so $\ell \mid (p-1)!$. Also,

$$\ell \mid p \mid ((p-1)! - 1).$$

This is a contradiction, because a prime can't divide a number a and also divide $a-1$, since it would then have to divide $a-(a-1)=1$. □

Example 1.3. When $p=17$, we have

$$2 \cdot 3 \cdot \cdots \cdot 15 = (2\cdot 9)\cdot(3\cdot 6)\cdot(4\cdot 13)\cdot(5\cdot 7)\cdot(8\cdot 15)\cdot(10\cdot 12)\cdot(14\cdot 11) \equiv 1 \pmod{17},$$

where we have paired up the numbers a, b for which $ab \equiv 1 \pmod{17}$.

Let's test Wilson's Theorem in PARI:

```
? wilson(n) = Mod((n-1)!,n) == Mod(-1,n)
? wilson(5)
%9 = 1
? wilson(10)
%10 = 0
? wilson(389)
%11 = 1
? wilson(2001)
%12 = 0
```

Warning: In practice, this is a horribly inefficient way to check whether or not a number is prime.

2 The Chinese Remainder Theorem

Sun Tsu Suan-Ching (4th century AD):

> There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

In modern notation, Sun is asking us to solve the following system of equations:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

The Chinese Remainder Theorem asserts that a solution to Sun's question exists, and the proof gives a method to find a solution.

Theorem 2.1 (The Chinese Remainder Theorem). *Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N}$ such that* $\gcd(n, m) = 1$. *Then there exists $x \in \mathbb{Z}$ such that*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Proof. The equation

$$tm \equiv b - a \pmod{n}$$

has a solution t since $\gcd(m, n) = 1$. Set $x = a + tm$. We next verify that x is a solution to the two equations. Then

$$x \equiv a + (b - a) \equiv b \pmod{n},$$

and

$$x = a + tm \equiv a \pmod{m}.$$

□

Now we can solve Sun's problem:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

First, we use the theorem to find a solution to the pair of equations

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

Set $a = 2$, $b = 3$, $m = 3$, $n = 5$. Step 1 is to find a solution to $t \cdot 3 \equiv 3 - 2 \pmod{5}$. A solution is $t = 2$. Then $x = a + tm = 2 + 2 \cdot 3 = 8$. Since any x' with $x' \equiv x \pmod{15}$ is also a solution to those two equations, we can solve all three equations by finding a solution to the pair of equations

$$\begin{aligned} x &\equiv 8 \pmod{15} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

Again, we find a solution to $t \cdot 15 \equiv 2 - 8 \pmod{7}$. A solution is $t = 1$, so

$$x = a + tm = 8 + 15 = 23.$$

Note that there are other solutions. Any $x' \equiv x \pmod{3 \cdot 5 \cdot 7}$ is also a solution; e.g., $23 + 3 \cdot 5 \cdot 7 = 128$.

We can also solve Sun's problem in PARI:

```
? chinese(Mod(2,3),Mod(3,5))
%13 = Mod(8, 15)
? chinese(Mod(8,15),Mod(2,7))
%14 = Mod(23, 105)
```

3 Multiplicative Functions

Definition 3.1. A function $f : \mathbb{N} \to \mathbb{Z}$ is *multiplicative* if, whenever $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$, we have

$$f(mn) = f(m) \cdot f(n).$$

Recall that the *Euler φ-function* is

$$\varphi(n) = \#\{a : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}.$$

Proposition 3.2. *φ is a multiplicative function.*

Proof. Suppose that $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Consider the map

$$\{c : 1 \leq c \leq mn \text{ and } \gcd(c, mn) = 1\} \xrightarrow{f}$$
$$\{a : 1 \leq a \leq m \text{ and } \gcd(a, m) = 1\} \times \{b : 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}\}$$

defined by

$$f(c) = (c \bmod m, \quad c \bmod n).$$

The map f is injective: If $f(c) = f(c')$, then $m \mid c - c'$ and $n \mid c - c'$, so, since $\gcd(n, m) = 1$, $nm \mid c - c'$, so $c = c'$.

The map f is surjective: Given a, b with $\gcd(a, m) = 1$, $\gcd(b, n) = 1$, the Chinese Remainder Theorem implies that there exists c with $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$. We may assume that $1 \leq c \leq nm$, ans since $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$, we must have $\gcd(c, nm) = 1$. Thus $f(c) = (a, b)$.

Because f is a bijection, the set on the left has the same size as the product set on the right. Thus

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

□

Example 3.3. The proposition makes it easier to compute $\varphi(n)$. For example,

$$\varphi(12) = \varphi(2^2) \cdot \varphi(3) = 2 \cdot 2 = 4.$$

Also, for $n \geq 1$, we have

$$\varphi(p^n) = p^n - \frac{p^n}{p},$$

since $\varphi(p^n)$ is the number of numbers less than p^n minus the number of those that are divisible by p. Thus, e.g.,

$$\varphi(389 \cdot 11^2) = 388 \cdot (11^2 - 11) = 388 \cdot 110 = 42680.$$

The φ function is also available in PARI:

```
? eulerphi(389*11^2)
%15 = 42680
```

Question 3.4. Is computing φ(1000 digit number) really easy or really hard?