MAT246H1S Lec0101 Burbulla

Chapter 5 Lecture Notes
Fermat's Theorem and Wilson's Theorem

Winter 2019

Congruency Modulo p

Let p be a prime number. Congruency modulo p has many interesting properties, compared to congruency modulo m, for m composite. For example, consider multiplication modulo 7 :

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Every $r \in \{1, 2, 3, 4, 5, 6\}$ has a 'reciprocal' in $\{1, 2, 3, 4, 5, 6\}$: $1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 4^{-1} = 2, 5^{-1} = 3,$ and $6^{-1} = 6$.

Compare with multiplication modulo 6 :

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

In this case we can write $1^{-1} = 1$ and $5^{-1} = 5$; but the other non-zero numbers in $\{1, 2, 3, 4, 5\}$, namely $2, 3$ and 4, are divisors of zero:

$$2 \cdot 3 \equiv 0 \pmod{6} \text{ and } 3 \cdot 4 \equiv 0 \pmod{6}.$$

In practice, this means that it will be much easier to solve congruencies modulo p, where p is prime, than it will be to solve congruencies modulo m, where m is composite.

Theorem 5.1.1

First we find conditions under which "cancelling" common factors is valid, modulo p.

Theorem: Let p be a prime and suppose that a is not divisible by p. If $ab \equiv ac \pmod{p}$, then $b \equiv c \pmod{p}$.

Proof: $ab \equiv ac \pmod{p}$ means that $p \mid (ab - ac)$. Factoring gives

$$p \mid a(b-c).$$

Since p is prime, $p \mid a$ or $p \mid b-c$. But we are given that p does *not* divide a, so we must have

$$p \mid b-c \Leftrightarrow b \equiv c \pmod{p}.$$

Fermat's Theorem

Theorem 5.1.2: if p is a prime number and a is any natural number not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: recall that no two numbers in the set $\{1, 2, \ldots, p-1\}$ are equivalent modulo p to each other. And if p does not divide a then neither are any two numbers in the set $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$, by Theorem 5.1.1. On the other hand, since p does not divide a nor any of the numbers $1, 2, \ldots, p-1$, each of the numbers in the set $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$ is congruent to exactly one number in the set $\{1, 2, \ldots, p-1\}$, by Theorem 3.1.4. Thus

$$a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) = a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Now use Theorem 5.1.1, repeatedly, to cancel $2, 3, \ldots, p-1$ and conclude that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Example 1

What is the remainder of 7^{8152} when divided by 13?

Solution: by Fermat's Theorem $7^{12} \equiv 1 \pmod{13}$. Note that $8152 = 679 \cdot 12 + 4$. Thus

$$\begin{aligned} 7^{8152} = (7^{12})^{679} \cdot 7^4 &\equiv 1^{679} \cdot 7^4 \pmod{13} \\ &\equiv 1 \cdot 7^4 \pmod{13} \\ &\equiv (49)^2 \pmod{13} \\ &\equiv (10)^2 \pmod{13} \\ &\equiv (-3)^2 \pmod{13} \\ &\equiv 9 \pmod{13}. \end{aligned}$$

So the remainder is 9.

Two Corollaries

Corollary 5.1.3: if p is a prime number and a is any natural number, then $a^p \equiv a \pmod{p}$.

Proof: if $a \equiv 0 \pmod{p}$, then $a^p \equiv 0 \pmod{p}$ as well, and the equation holds. If p does not divide a, then by Fermat's Theorem

$$a^{p-1} \equiv 1 \pmod{p}, \text{ implying } a^p \equiv a \pmod{p}.$$

Corollary 5.1.5: if p is a prime and a is any natural number not divisible by p, then there is a natural number x such that $a \cdot x \equiv 1 \pmod{p}$.

Proof: if $p = 2$ then a must be odd, and $x = 1$ will do. If $p > 2$, let $x = a^{p-2}$ and use Fermat's Theorem:

$$a \cdot x = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}.$$

Multiplicative Inverses, Modulo p

Definition 5.1.4: a *multiplicative inverse modulo p* for a natural number a is a natural number b such that $a \cdot b \equiv 1 \pmod{p}$.

- Corollary 5.1.5 says that any natural number a not divisible by p has a multiplicative inverse modulo p. For example, if $p = 7$, then the example at the beginning of this section showed that the multiplicative inverse of 2 is 4, and that the multiplicative inverse of 3 is $5 : 2 \cdot 4 = 8 \equiv 1 \pmod{7}$ and $3 \cdot 5 = 15 \equiv 1 \pmod{7}$.
- Natural numbers can have inverses modulo m, if m is composite, but need not. For example, if $m = 6$ we saw that 2 has no multiplicative inverse modulo 6, but that 5 has a multiplicative inverse, namely itself: $5 \cdot 5 = 25 \equiv 1 \pmod{6}$.

When Is a Multiplicative Inverse Equal to Itself?

Theorem 5.1.7: if p is a prime number and x is an integer satisfying $x^2 \equiv 1 \pmod{p}$, then $x \equiv \pm 1 \pmod{p}$.

Proof: we use Corollary 4.1.3.

$$\begin{aligned} x^2 \equiv 1 \pmod{p} \quad &\Rightarrow \quad p \mid (x^2 - 1) = (x-1)(x+1) \\ &\Rightarrow \quad p \mid x - 1 \text{ or } p \mid x + 1 \\ &\Rightarrow \quad x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \pmod{p} \end{aligned}$$

Note: $-1 \equiv p - 1 \pmod{p}$, so Corollary 4.1.3 can also be stated as

$$x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv 1 \pmod{p} \text{ or } x \equiv p - 1 \pmod{p}.$$

Lemma 5.1.6

This lemma will be useful in the proof of Wilson's Theorem.

Lemma 5.1.6: let p be a prime. If a and c have the same multiplicative inverse modulo p, then $a \equiv c \pmod{p}$.

Proof: suppose $a \cdot b \equiv 1 \pmod{p}$ and $c \cdot b \equiv 1 \pmod{p}$. Then

$$\begin{aligned} c \cdot b \equiv 1 \pmod{p} \quad &\Rightarrow \quad c \cdot b \cdot a \equiv 1 \cdot a \pmod{p} \\ &\Rightarrow \quad c(b \cdot a) \equiv a \pmod{p} \\ &\Rightarrow \quad c \cdot 1 \equiv a \pmod{p} \\ &\Rightarrow \quad c \equiv a \pmod{p} \end{aligned}$$

Comment: aside from this lemma, there are other observations that will be useful in proving Wilson's Theorem. They can all be stated as properties of the set $R = \{1, 2, \ldots, p-2, p-1\}$.

Properties of the Set $R = \{1, 2, \ldots, p-2, p-1\}$

- 1: $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1)$, the product of all the elements in R.
- 2: every number in R is distinct, modulo p, as we saw in the proof of Theorem 3.1.3.
- 3: each number in R has a multiplicative inverse, modulo p, by Corollary 5.1.5.
- 4: the multiplicative inverse of each number in R is congruent to one of the numbers in R, by Theorem 3.1.4.
- 5: by Lemma 5.1.6, no two distinct numbers in R can have the same multiplicative inverse.
- 6: 1 and $p-1$ are the only numbers in R that are their own multiplicative inverses, by Theorem 5.1.7.

- 7: each number in the set $\{2, 3, \ldots, p-3, p-2\}$ has a multiplicative inverse in that set, and the number differs from its multiplicative inverse.
- 8: if x is the multiplicative inverse of y, then y is the multiplicative inverse of x, and vice-versa; thus the numbers in the set $\{2, 3, \ldots, p-3, p-2\}$ come in pairs, each pair of which consists of numbers that are multiplicative inverses of each other.
- 9: the product of all the numbers in the set

$$\{2, 3, \ldots, p-3, p-2\}$$

is congruent to 1, modulo p, by item 8.

We now have enough facts to prove Wilson's Theorem; the key one is Item 9.

Wilson's Theorem

Theorem 5.2.1: if p is prime then $(p-1)! + 1 \equiv 0 \pmod{p}$.

Proof: if $p = 2$ the theorem is obviously true. Now assume $p > 2$.

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdots (p-2) \cdot (p-1) \\
&\equiv 1 \cdot \underbrace{2 \cdots (p-2)}_{\text{congruent to } 1} \cdot (p-1) \pmod{p} \\
&\equiv (p-1) \pmod{p} \\
&\equiv -1 \pmod{p} \\
\Rightarrow (p-1)! + 1 &\equiv 0 \pmod{p}
\end{aligned}$$

Example: for example, if $p = 7$, $6! + 1 = 721 \equiv 0 \pmod{7}$.

Theorem 5.2.2

What happens to the conclusion of Wilson's Theorem if m is composite? We obtain a very different result:
Theorem: if m is a composite number larger than 4, then $(m-1)! \equiv 0 \pmod m$; that is, $(m-1)! + 1 \equiv 1 \pmod m$.

Proof: let $m = a \cdot b$, where $1 < a, b < m$. There are two cases:

1. $a \neq b$: then a and b both divide $(m-1)!$, so $ab \mid (m-1)!$ and $(m-1)! \equiv 0 \pmod m$.
2. $a = b$: then $m = a^2$. If a is not prime, then we can reduce this case to case 1. If $a = p$, for p prime, then $m = p^2$ and $p > 2$, because $m > 4$. In particular $m = p^2 > 2p > p$. Then

$$(m-1)! = (p^2-1)! = 1 \cdot 2 \cdots p \cdots 2p \cdots (p^2-1),$$

implying $2p^2 \mid (m-1)! \Rightarrow m = p^2 \mid (m-1)!$
and so $(m-1)! \equiv 0 \,(\text{mod } m)$.

Theorem 5.2.3

We can combine Wilson's Theorem and its converse:
Theorem: if m is a natural number other than 1, then $(m-1)! + 1 \equiv 0 \pmod m$ if and only if m is a prime number.

Proof: $(\Leftarrow)$ if m is prime, then $(m-1)! + 1 \equiv 0 \pmod m$ is true by Wilson's theorem.
$(\Rightarrow)$ if m is *not* prime and $m > 4$, then by Theorem 5.2.2,

$$(m-1)! + 1 \equiv 1 \pmod m,$$

and $(m-1)! + 1$ is *not* congruent to 0, modulo m. Finally, if $m = 4$, then $(m-1)! + 1 = 3! + 1 = 7 \equiv 3 \pmod 4$.

Comment: even though this theorem gives a computational condition to test if m is prime, it is not a practical condition because $(m-1)! + 1$ can be very large!