

## 6 Special Congruences

### 6.1 Wilson's Theorem & Fermat's Little Theorem

---

1. **Wilson's Theorem:** If  $p$  is prime then

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

*Proof.* The case where  $p = 2$  is trivial to show, so let's look at primes  $p \geq 3$ . Consider the set of numbers  $\underbrace{\{1, 2, 3, 4, 5, \dots, p-1\}}_{\text{even number of integers}}$ . Suppose  $a$  is one of

these, then  $\exists b \in \mathbb{Z}$  such that  $ab \equiv 1 \pmod{p}$  (a multiplicative inverse). Because the equation  $ax \equiv 1 \pmod{p}$  has one solution because  $\gcd(a, p) = 1 \mid 1$ . Note that  $\gcd(a, p) = 1$  because  $a$  is one of  $\{1, 2, 3, \dots, p-1\}$ .

Could we have, for some  $a \in \{1, 2, 3, \dots, p-1\}$  that  $a^2 \equiv 1 \pmod{p}$ ? Suppose  $a^2 \equiv 1 \pmod{p}$ , then  $p \mid a^2 - 1$  so  $p \mid (a+1)(a-1)$ , either  $p \mid (a+1)$  or  $p \mid (a-1)$ . If  $p \mid (a+1)$  then  $a \equiv -1 \pmod{p}$  or  $a \equiv p-1 \pmod{p}$ . If  $p \mid (a-1)$  then  $a \equiv 1 \pmod{p}$ .

**Ex.** Suppose  $p = 11$ , the set is  $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ . Then the respective pairs would be  $2 \cdot 6$ ,  $3 \cdot 4$ ,  $5 \cdot 9$ , and  $7 \cdot 8$ . Notice that 1 and 10 do not have a pair that results in congruence  $\pmod{11}$ .

In general in  $\{1, 2, 3, \dots, p-1\}$  the integers all pair up such that their products are congruent  $1 \pmod{p}$ , except for 1 and  $p-1$ . Thus,

$$(p-1)! = (1)(2)(3) \cdots (p-1) \equiv p-1 \equiv -1 \pmod{p}$$

□

**Ex.** Find the least non-negative residue of  $20! \pmod{23}$ .

Note: We see  $20!$  and think  $20! \equiv -1 \pmod{21}$ , but 21 is not prime so there is no guarantee and it does not apply anyways because we have  $\pmod{23}$ .

However,  $22! \equiv -1 \pmod{23}$

$$22! \equiv -1 \pmod{23}$$

$$(22)(21)(20!) \equiv -1 \pmod{23}$$

$$(-1)(-2)(20!) \equiv -1 \pmod{23}$$

$$(2)(20!) \equiv -1 \pmod{23}$$

$$(2)(20!) \equiv 22 \pmod{23}$$

$$20! \equiv 11 \pmod{23}$$

In this case, 11 is the least non-negative residue.

2. **Fermat's Little Theorem:** Suppose  $p$  is prime and  $a \in \mathbb{Z}$  with  $p \nmid a$ . Then,

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

**Ex.**  $p = 97$  and  $a = 10$ , so  $10^{96} \equiv 1 \pmod{97}$ .

*Proof.* Consider the set of integers  $S = \{a, 2a, 3a, \dots, (p-1)a\}$  (there are  $p-1$  integers in this set).

- First observe that none are congruent  $0 \pmod{p}$  because if  $p \mid ka$  for some  $1 \leq k \leq (p-1)$ . Then  $p \mid k$  or  $p \mid a$  but  $p \nmid a$  so  $p \mid k$  but  $1 \leq k \leq p-1$ .
- Second, no two are congruent one another  $\pmod{p}$  because if  $k_1a \equiv k_2a \pmod{p}$  for some  $1 \leq k_1 \leq p-1$  and  $1 \leq k_2 \leq p-1$ . Then  $p \mid (k_1a - k_2a) = p \mid a(k_1 - k_2)$ , since  $p \nmid a$  then  $p \mid (k_1 - k_2)$ . But this is impossible because  $1 - (p-1) \leq k_1 - k_2 \leq (p-1) - 1$ .

Thus the set  $S$ , is we take all  $\pmod{p}$ , is equivalent to the set  $T = \{1, 2, 3, \dots, p-1\}$  in some order. Since,  $\pmod{p}$ , all the numbers in  $S$  is congruent to all the numbers in  $T$ , we have

$$\begin{aligned} (a)(2a)(3a) \cdots ((p-1)a) &\equiv (1)(2)(3) \cdots (p-1) \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1}(-1) &\equiv (-1) \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

Notice that we can cancel all of the  $1, 2, 3, \dots, p-1$  without affecting the modulus because they are coprime to  $p$ .  $\square$

**Ex.** Find the least non-negative residue of  $5^{123} \pmod{13}$ .

Well  $13 \nmid 5$  so  $5^{12} \equiv 1 \pmod{13}$ . Then  $123 = 12(10) + 3$  so

$$\begin{aligned} 5^{123} &= 5^{12(10)+3} = 5^{12^{10}}5^3 \equiv (1)^{10}5^3 \pmod{13} \\ &\equiv 5^3 \pmod{13} \\ &\equiv 5 \cdot 25 \pmod{13} \\ &\equiv 5(-1) \pmod{13} \\ &\equiv -5 \pmod{13} \\ &\equiv 8 \pmod{13} \end{aligned}$$

So 8 is the least non-negative residue.

**Corollary:** From  $a^{p-1} \equiv 1 \pmod{p}$  we get  $a^p \equiv a \pmod{p}$ . Note that  $a^p \equiv a \pmod{p}$  even when  $p \mid a$  because if  $p \mid a$  then  $a \equiv 0 \pmod{p}$  and  $a^p \equiv a \pmod{p}$  is saying  $0 \equiv 0 \pmod{p}$ .

3. **Closing Notes:** This is relevant to cryptography for one of two reasons.

- Encryption (which involved big exponents) is both practical and theoretically possible based on Fermat's Little Theorem and Euler's Theorem.
- Pseudoprime is a non-prime which "behaves like a prime". e.g. in FLiT maybe  $p$  is not prime but still when  $p \nmid a$  we get  $a^{p-1} \equiv 1 \pmod{p}$ .

## 6.2 Fermat Pseudoprimes & Carmichael Numbers

---

1. **Introduction:** Primes are useful. Given  $n \in \mathbb{Z}^+$  how can we check if  $n$  is prime? We could divide by everything (computationally intensive). Or we could use some tests which give insight.

2. **Fermat Pseudoprimes:**

- (a) **Reminder:** FLiT: If  $p$  is prime and  $p \nmid a$  then  $a^{p-1} \equiv 1 \pmod{p}$ . Suppose we have some  $n \in \mathbb{Z}$  with  $n \geq 2$ . Suppose we find some  $a$  with  $n \nmid a$  and  $a^{n-1} \not\equiv 1 \pmod{n}$ . We can conclude that  $n$  is not prime.

**Ex:** Let  $n = 63$ , observe that if  $a = 2$  then  $n \nmid a$  clearly and  $2^{62} \equiv 4 \not\equiv 1 \pmod{63}$ . Thus, 63 is not prime.

**Definition:**  $a = 2$  is a *Fermat Witness* to the fact that 63 is composite.

However, we might have some  $n$  and  $a$  with  $n \nmid a$  and  $a^{n-1} \equiv 1 \pmod{n}$  but still have  $n$  composite.

**Ex.** Let  $n = 341$  and  $a = 2$ , then  $341 \nmid 2$  and observe

$$2^{340} \equiv 1 \pmod{341}$$

Even though  $n = 341 = 11 \cdot 31$  is not prime it still "passes Fermat's Little Theorem with  $a = 2$ ."

**Definition:**  $a = 2$  is a *Fermat Liar* for  $n = 341$ .

- (b) **Definition:** Suppose  $n$  is composite and  $b \in \mathbb{Z}$  satisfies  $\gcd(n, b) = 1$  and  $b^{n-1} \equiv 1 \pmod{n}$ . Then we say  $n$  is a *Fermat Pseudoprime to the base  $b$* .

**Ex:** So 341 is a *Fermat Pseudoprime with the base  $b = 2$* .

**Ex:** Likewise, 645 is a *Fermat Pseudoprime with the base  $b = 2$* .

3. **Carmichael Numbers:**

- (a) **Introduction:** Given some  $n$  we wish to test if it is prime.
- Pick some  $b$  with  $\gcd(b, n) = 1$ . Suppose we find  $b^{n-1} \equiv 1 \pmod{n}$ . Either  $n$  is prime or  $b$  is a liar and  $n$  is a Fermat Pseudoprime with base  $b$ .
  - Try another  $b$  with  $\gcd(b, n) = 1 \dots$

So, is it possible that we could try all  $b$  with  $\gcd(b, n) = 1$  and always get  $b^{n-1} \equiv 1 \pmod n$  and still have a composite  $n$ ? The answer, yes!

- (b) **Definition:** A number  $n$  is a *Carmichael Number* if it is a Fermat Pseudoprime for every base  $b$  with  $\gcd(b, n) = 1$ . These are sometimes called Absolute Pseudoprimes.

**Ex:**  $n = 561$  is a Carmichael Number. Note that  $561 = 3 \cdot 11 \cdot 17$ . Suppose  $b$  satisfies  $\gcd(b, 561) = 1$ . Then

- $\gcd(b, 3) = 1$  so by FLiT  $b^2 \equiv 1 \pmod 3$ . So  $b^{560} = (b^2)^{280} \equiv 1 \pmod 3$  so  $3 \mid b^{560} - 1$ .
- $\gcd(b, 11) = 1$  so by FLiT  $b^{10} \equiv 1 \pmod{11}$ . So  $b^{560} = (b^{10})^{56} \equiv (1)^{56} \equiv 1 \pmod{11}$  so  $11 \mid b^{560} - 1$ .
- $\gcd(b, 17) = 1$  so by FLiT  $b^{16} \equiv 1 \pmod{17}$ . So  $b^{560} = (b^{16})^{35} \equiv (1)^{35} \equiv 1 \pmod{17}$  so  $17 \mid b^{560} - 1$ .

So  $3 \cdot 11 \cdot 17 \mid b^{560} - 1 \implies 561 \mid b^{560} - 1$ . Therefore  $b^{560} \equiv 1 \pmod{561}$ .

- (c) **Theorem:** Suppose  $n = p_1 p_2 \cdots p_k$  such that  $\forall i$  we have  $p_i - 1 \mid n - 1$ . Then  $n$  is a Carmichael Number.

*Proof.* Suppose  $\gcd(b, n) = 1$ . Claim that  $b^{n-1} \equiv 1 \pmod n$  well, for each  $i$  we have  $\gcd(b, p_i) = 1$ . By FLiT we have  $b^{p_i-1} \equiv 1 \pmod{p_i}$  then  $b^{n-1} = b^{\alpha(p_i-1)} \equiv (1)^\alpha \equiv 1 \pmod{p_i}$ . Thus,  $p_i \mid b^{n-1} - 1$  for all  $i$ . Therefore,  $n \mid b^{n-1} - 1$  so  $b^{n-1} \equiv 1 \pmod n$ .  $\square$

## 6.3 Euler's Theorem

---

1. **Introduction:** Fermat's Little Theorem tells us that if  $p$  is a prime and if  $p \nmid a$  then  $a^{p-1} \equiv 1 \pmod p$ . This is relevant for both calculation and cryptography. Since this is useful for reducing large powers of  $a \pmod p$  it might be helpful if we had a version for when the modulus is not prime.

### 2. Preliminaries:

- (a) **Definition:** Define the *Euler Phi-Function*  $\phi : \mathbb{Z}^+ \rightarrow \mathbb{Z}$ . For  $n \in \mathbb{Z}^+$  we define  $\phi(1) = 1$  and  $\phi(n)$  = the number of positive integers less than  $n$  which are coprime to  $n$ .

**Ex.**  $\phi(10) = 4$  because the set  $\{1, 3, 7, 9\}$  is all coprime to 10.

**Ex.**  $\phi(97) = 96$  because  $\{1, 2, \dots, 96\}$  are all coprime to 96.

**Definition:** If  $n$  is prime then  $\phi(n) = n - 1$ .

- (b) **Recall:** A complete residue system mod  $n$  is a set of  $n$  integers, none of them congruent to each other mod  $n$ . CRS mod 8 is  $\{0, 1, 2, \dots, 7\}$ .

- (c) **Definition:** A *reduced residue system* mod  $n$  is a set of  $\phi(n)$  integers all of which are coprime to  $n$  and no two of which are congruent to each other mod  $n$ .

**Ex.** RRS mod 10 is  $\{1, 3, 7, 9\}$  or  $\{11, -7, 7, 29\}$ .

- (d) **Theorem:** Suppose  $\{r_1, r_2, \dots, r_{\phi(n)}\}$  is a RRS mod  $n$ . Then suppose  $a \in \mathbb{Z}$  with  $\gcd(a, n) = 1$ . Then  $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$  is also a RRS mod  $n$ .

*Proof.* We see there are  $\phi(n)$  of them. Claim that each is coprime to  $n$ .

- By means of contradiction, suppose we have some  $ar_i$  not coprime to  $n$ , that is  $\gcd(ar_i, n) \neq 1$ . Then  $\exists$  a prime  $p$  with  $p \mid ar_i$  and  $p \mid n$ . Since  $p \mid ar_i$  so  $p \mid a$  or  $p \mid r_i$ . If  $p \mid a$  then, along with  $p \mid n$ , we have a contradiction because  $\gcd(a, n) = 1$ . If  $p \mid r_i$  then, along with  $p \mid n$ , we have a contradiction because  $\gcd(r_i, n) = 1$ . So the  $ar_i$  are coprime to  $n$ .
- Suppose we have  $ar_i \equiv ar_j \pmod{n}$ , since  $\gcd(a, n) = 1$  we can cancel. So  $r_i \equiv r_j \pmod{n}$ . So no two new elements are congruent mod  $n$ .

□

3. **Euler's Theorem:** Suppose  $n$  is a modulus and  $\gcd(a, n) = 1$ . Then  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**Note.** If  $n = p = \text{prime}$  we have  $\phi(n) = n - 1$  and we get Fermat's Little Theorem.

*Proof.* Given a modulus  $n$ , let  $S = \{r_1, \dots, r_{\phi(n)}\}$  be any RRS. Then by the theorem above,  $S' = \{ar_1, \dots, ar_{\phi(n)}\}$  is also a RRS. It follows that  $S$  and  $S'$  consist of the same integers mod  $n$ . Thus,

$$(ar_1)(ar_2) \cdots (ar_{\phi(n)}) \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

□

4. **Use For Calculation:** To reduce  $9^{453} \pmod{16}$ , we note that  $\gcd(9, 16) = 1$  so Euler's Theorem tells us that  $9^{\phi(16)} \equiv 1 \pmod{16}$ . Since  $\phi(16) = 8$  we have  $9^8 \equiv 1 \pmod{16}$  and so:

$$9^{453} = 9^{8(56)+5} \equiv 9^5 \equiv 9(81)^2 \equiv 9 \pmod{16}$$

5. **Note:** If  $\gcd(a, n) = 1$  then  $a^{\phi(n)-1}$  is a multiplicative inverse of  $a \pmod{n}$ .

## 6.4 Problems

---

1. Use Fermat's Little Theorem to find the least nonnegative residue of  $2^{1000003} \pmod{17}$ .
2. Use Fermat's Little Theorem to solve the following, giving the result as the least nonnegative residue.
  - (a)  $7x \equiv 12 \pmod{17}$
  - (b)  $10x \equiv 13 \pmod{19}$
3. Use Fermat's Little Theorem to show that  $30 \mid (n^9 - n)$  for all positive integers  $n$ .
4. The definition of  $n$  being a Fermat pseudoprime to base  $b$  does not actually require that  $\gcd(b, n) = 1$  because it's not possible to have  $b^{n-1} \equiv 1 \pmod{n}$  with  $\gcd(b, n) \neq 1$ . Prove this.
5. We didn't exclude even integers from the definition of a Fermat Pseudoprime. Some books do. Show that with our definition 4 is a Fermat Pseudoprime to a certain base.
6. Prove that if  $n$  is an odd Fermat Pseudoprime to some base then it must be so to an even number of bases.
7. Prove that 1105 is a Carmichael number.
8. Use Euler's Theorem to find the units digit of  $7^{999999}$ .
9. Solve each of the following using Euler's Theorem. Solutions should be least nonnegative residues.
  - (a)  $5x \equiv 3 \pmod{14}$
  - (b)  $4x \equiv 7 \pmod{15}$
  - (c)  $3x \equiv 5 \pmod{16}$
10. Prove that if  $\gcd(a, 30) = 1$  then  $60 \mid a^4 + 59$ .