1 Special Congruences

1.1 Wilson's Theorem & Fermat's Little Theorem

---

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

$$(p-1)! \equiv -1 \mod p$$

Proof. The case where $p = 2$ is trivial to show, so let's look at primes $p \geq 3$. Consider the set of numbers $\underbrace{\{1, 2, 3, 4, 5, \cdots, p-1\}}_{\text{even number of integers}}$. Suppose a is one of these, then $\exists b \in \mathbb{Z}$ such that $ab \equiv 1 \mod p$ (a multiplicative inverse). Because the equation $ax \equiv 1 \mod p$ has one solution because $\gcd(a, p) = 1 \mid 1$. Note that $\gcd(a, p) = 1$ because a is one of $\{1, 2, 3, \cdots, p-1\}$.
Could we have, for some $a \in \{1, 2, 3, \cdots, p-1\}$ that $a^2 \equiv 1 \mod p$?
Suppose $a^2 \equiv 1 \mod p$, 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 $a \equiv -1 \mod p$ or $a \equiv p-1 \mod p$. If $p \mid (a-1)$ then $a \equiv 1 \mod p$.

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 $\mod 11$.

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

$$(p-1)! = (1)(2)(3)\cdots(p-1) \equiv p-1 \equiv -1 \mod p$$

$\square$

Ex. Find the least non-negative residue of $20! \mod 23$.
Note: We see $20!$ and think $20! \equiv -1 \mod 21$, but 21 is not prime so there is no guarantee and it does not apply anyways because we have $\mod 23$.
However, $22! \equiv -1 \mod 23$

$$\begin{aligned}
22! &\equiv -1 \mod 23 \\
(22)(21)(20!) &\equiv -1 \mod 23 \\
(-1)(-2)(20!) &\equiv -1 \mod 23 \\
(2)(20!) &\equiv -1 \mod 23 \\
(2)(20!) &\equiv 22 \mod 23 \\
20! &\equiv 11 \mod 23
\end{aligned}$$

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,

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

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

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

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

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

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

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

Ex. Find the least non-negative residue of $5^{123} \mod 13$.
Well $13 \nmid 5$ so $5^{12} \equiv 1 \mod 13$. Then $123 = 12(10) + 3$ so

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

So 8 is the least non-negative residue.

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

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

1.2 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. **Femat Pseudoprimes:**
   (a) **Reminder:** FLiT: If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$. Suppose we have some $n \in \mathbb{Z}$ with $n \geq 2$. Suppose we find some a with $n \nmid a$ and $a^{n-1} \not\equiv 1 \mod n$. We can conclude that n is not prime.
   Ex: Let $n = 63$, observe that if $a = 2$ then $n \nmid a$ clearly and $2^{62} \equiv 4 \not\equiv 1 \mod 63$. 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 $a^{n-1} \equiv 1 \mod n$ but still have n composite.
   Ex. Let $n = 341$ and $a = 2$, then $341 \nmid 2$ and observe
   $$2^{340} \equiv 1 \mod 341$$
   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 $\gcd(n, n) = 1$ and $b^{n-1} \equiv 1 \mod n$. 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 $b^{n-1} \equiv 1 \mod n$. Either n is prime or b is a liar and n is a Fermat Pseudoprime with base b.
   - Try another b with $\gcd(b, n) = 1 \cdots$

   So, is it possible that we could try all b with $\gcd(b, n) = 1$ and always get $b^{n-1} \equiv 1 \mod n$ 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 $b^2 \equiv 1 \mod 3$. So $b^{560} = (b^2)^{280} \equiv 1 \mod 3$ so $3 \mid b^{560} - 1$.
- $\gcd(b, 11) = 1$ so by FLiT $b^{10} \equiv 1 \mod 11$. So $b^{560} = (b^{10})^{56} = (1)^{56} \equiv 1 \mod 11$ so $11 \mid b^{560} - 1$.
- $\gcd(b, 17) = 1$ so by FLiT $b^{16} \equiv 1 \mod 17$. So $b^{560} = (b^{16})^{35} \equiv (1)^{35} \equiv 1 \mod 17$ so $17 \mid b^{560} - 1$.

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

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