Number Theory Section Summary: 5.4
Wilson's Theorem

1. Summary

   Wilson's theorem provides a mechanism for detecting whether an integer is prime, but because of the factorial function involved, is practically useless! Factorials grow so fast that the numbers involved spin rapidly into the stratosphere....

   Check out the interesting story behind this theorem! The comment by Gauss is especially amusing: "notationes versus notiones...." – Can't you just see the great man grumbling?! Then to have Lagrange and Leibniz tied up with the theorem....

2. **Theorems**

   Theorem 5.4 (Wilson's Theorem): If p is prime, then

   $$(p-1)! \equiv -1 (\text{mod p})$$

   Exercise #1, p. 101

   Converse to Wilson's Theorem): If

   $$\overline{(p-1)! \equiv -1 (\text{mod p})}$$

   then p is prime.

   Exercise #2, p. 101

   Theorem 5.5: The quadratic congruence $x^2 + 1 \equiv 0 (\text{mod p})$, where p is an odd prime, has a solution if and only if $p \equiv 1 (\text{mod } 4)$.

$p=2$

$1 \equiv -1 \pmod 2$

$p=3$

$2 \equiv -1 \pmod 3$

$p=5$

$24 \equiv -1 \pmod 5$

3. Properties/Tricks/Hints/Etc.

   Once again we make good use of the result that

   $a \equiv b (\text{mod n})$ and $a \equiv b (\text{mod m})$ with gcd(n,m)=1 $\Longrightarrow a \equiv b (\text{mod mn})$

   Exercise #6, p. 101

Wilson's Theorem:

Proof (direct)

Checked for $p=2$ and $p=3$.

Consider $p > 3$.

Let $a \in \{1, \dots, p-1\}$ (an even # of values)

& consider the linear congruence

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

Because $\gcd(a, p) = 1$, this has a unique solution, $x = a' \in \{1, \dots, p-1\}$.

$$a = a' \iff a = 1 \text{ or } a = p-1$$

since

$$a^2 \equiv 1 \pmod{p}$$

$$\iff (a^2 - 1) \equiv 0 \pmod{p}$$

$$\iff (a-1)(a+1) \equiv 0 \pmod{p}$$

$$\iff p \mid (a-1) \text{ or } p \mid (a+1)$$

either $a = 1$ or $a = p-1$

Consider $a \in \{2, \dots, p-2\}$.

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

has a unique solution a', & $a' \neq a$.

Remove that pair from the set, & iterate until all pairs have been removed.*

* $aa' \equiv a \cdot b' \pmod{p} \implies a' \equiv b' \pmod{p}$

since $\gcd(a,p)=1$.

Now multiply all the pairs together,

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

Hence
$$(p-1)! \equiv -1 \pmod p.$$

#1 p101

a. Find the remainder when $15!$ is divided by 17

[What's $15! \pmod{17}$?]

We know that
$$16! \equiv -1 \pmod{17}$$
by Wilson's theorem.
$$16\cdot 15! \equiv 16 \pmod{17}$$
so
$$15! \equiv \boxed{1} \pmod{17}$$

b. What's $2\cdot(26!) \pmod{29}$?

We know that
$$28! \equiv -1 \pmod{29}$$

$$28 \cdot 27 \cdot 26! \equiv -1 \pmod{29}$$

$$(-1)\cdot(-2)\cdot 26! \equiv -1 \pmod{29}$$

$$2\cdot(26!) \equiv \boxed{28} \equiv -1 \pmod{29}$$

#2 Can we show that

$$16! \equiv -1 \pmod{17}$$

(& hence conclude that 17 is prime by the converse to Wilson's Theorem?)

Consider $16! \equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12\cdot 13\cdot 14\cdot 15\cdot 16 \pmod{17}$

$$\equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot -8\cdot -7\cdot -6\cdot -5\cdot -4\cdot -3\cdot -2\cdot -1$$

$-1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1$

$$\equiv -1 \pmod{17}$$

#6 $$(p-1)! \equiv p-1 \pmod{\underbrace{1+2+\dots+(p-1)}_{\frac{(p-1)p}{2}}}$$

Consider $p \geq 5$.

$\frac{p-1}{2}$ & p are relatively prime

Show that the result holds mod p & mod $\frac{p-1}{2}$, & conclude that it holds mod $\frac{(p-1)p}{2}$.

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

$$p-1 \equiv -1 \pmod{p}, \quad \text{so}$$

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

Consider $\frac{p-1}{2}$.

$$p-1 = 2\left(\frac{p-1}{2}\right), \quad \text{so}$$

$$p-1 \equiv 0 \left(\bmod \frac{p-1}{2}\right) \quad \text{as is}$$

$$(p-1)! \equiv 0 \left(\bmod \frac{p-1}{2}\right); \quad \text{hence}$$

$$(p-1)! \equiv p-1 \left(\bmod \frac{p-1}{2}\right).$$

#14 p97

$$\underbrace{p^{q-1} + q^{p-1}}_{a} \equiv \underline{1} \pmod{pq}$$

$$\equiv b \pmod{pq}$$

Show $a \equiv b \pmod{p}$ [& invoke symmetry for q!] & we're done! Show:

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$$

$$p^{q-1} \equiv 0 \pmod{p},$$

so
$$q^{p-1} \equiv 1 \pmod{p} \ ?$$

Yes, by Fermat's little theorem.

#11, p101 Obtain two solutions to

$$x^2 \equiv -1 \pmod{29}$$

$$x^2 + 1 \equiv 0 \pmod{29}$$

$$29 = 1 + 4 \cdot 7$$
$$29 \equiv 1 \pmod{4} \ \checkmark$$

Let's construct a solution:

Consider
$$(p-1)! = \underline{1 \cdot 2 \cdot 3 \cdot \ldots \cdot \tfrac{p-1}{2}} \ \underline{\tfrac{p+1}{2}} \cdot \ldots \cdot (p-3)(p-2)(p-1)$$

$$p-1 \equiv -1 \bmod p$$
$$p-2 \equiv -2 \bmod p$$
$$\vdots$$
$$\tfrac{p+1}{2} \equiv -\tfrac{p-1}{2} \bmod p$$

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \tfrac{p-1}{2}\left(-\tfrac{p-1}{2}\right) \cdots (-3)(-2)(-1) \pmod{p}$$
$$\equiv (-1)^{\frac{p-1}{2}}\left[1 \cdot 1 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot \ldots \left(\tfrac{p-1}{2}\right)\left(\tfrac{p-1}{2}\right)\right]$$
$$\equiv (-1)^{\frac{p-1}{2}}\left[1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\tfrac{p-1}{2}\right)\right]^2$$
$$\equiv (-1)^{\frac{p-1}{2}}\left[\left(\tfrac{p-1}{2}\right)!\right]^2$$

p is of the form $p = 1 + 4n$, so

$$(-1)^{\frac{p-1}{2}} = (-1)^{4n/2} = (-1)^{2n} = 1$$

$$(p-1)! \equiv \left[\left(\tfrac{p-1}{2}\right)!\right]^2 \pmod{p}$$

$$\equiv -1 \pmod{p}$$ by Wilson's theorem, so

$$\boxed{\left[\left(\tfrac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 \pmod{p}}$$

So $\left(\frac{p-1}{2}\right)!$ is a solution to

$$x^2 + 1 \equiv 0 \pmod{p}$$

(as is $-\left(\frac{p-1}{2}\right)!$).

So $\left(\frac{29-1}{2}\right)! = 14!$ is a solution mod p.

$$14! \equiv 12 \pmod{29}$$

$$-14! \equiv -12 \equiv 17 \pmod{29}$$

are the two solutions.