5.4 Wilson's Theorem

Note Title 5/25/2005

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

Since $(17-1)! \equiv -1 \pmod{17}$, Then $16! \equiv -1 \pmod{17}$

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

$\therefore 16! \equiv 16 \pmod{17}$. $\gcd(16,17)=1$,

$\therefore 16!/16 \equiv 16/16 \pmod{17}$

$\therefore 15! \equiv 1 \pmod{17}$

(b) Find the remainder when $2(26!)$ is divided by 29

By Wilson's Th., $28! \equiv -1 \pmod{29}$

$\therefore 28! \equiv 28 \pmod{29}$, Since $\gcd(28,29)=1$,

$\therefore 27! \equiv 1 \pmod{29}$, $\therefore 27! \equiv 1+29 \pmod{29}$

$\therefore 27! \equiv 30 \pmod{29}$, $9 \cdot 3 \cdot 26! \equiv 30 \pmod{29}$,

$\therefore 9 \cdot 26! \equiv 10 \pmod{29}$ since $\gcd(3,29)=1$

$\therefore 9 \cdot 26! \equiv 39 \pmod{29}$

$3 \cdot 26! \equiv 13 \pmod{29}$

$\therefore 3 \cdot 26! \equiv 13+29 = 42 = 3 \cdot 14 \pmod{29}$

$\therefore 26! \equiv 14 \pmod{29}$, $\therefore \underline{2 \cdot 26! \equiv 28} \pmod{29}$

2. Determine whether 17 is a prime by deciding whether $16! \equiv -1 \pmod{17}$!

$4\cdot3\cdot2\cdot1 = 24 = 17+7 \equiv 7 \pmod{17}$

$\therefore 5! \equiv 5\cdot7 = 35 = 2\cdot17+1 \equiv 1 \pmod{17}$

$\therefore 6! \equiv 6 \pmod{17}$,

$7! \equiv 42 = 34+8 \equiv 8 \pmod{17}$

$8! \equiv 64 = 68-4 \equiv -4 \pmod{17}$

$9! \equiv -36 = -34-2 \equiv -2 \pmod{17}$

$10! \equiv -20 \equiv -3 \pmod{17}$

$11! \equiv -33 \equiv -34+1 \equiv 1 \pmod{17}$

$12! \equiv 12 = 17-5 \equiv -5 \pmod{17}$

$13! \equiv -5\cdot13 = -65 = -68+3 \equiv 3 \pmod{17}$

$14! \equiv 3\cdot14 = 42 = 34+8 \equiv 8 \pmod{17}$

$15! \equiv 8\cdot15 = 120 = 7\cdot17+1 \pmod{17}$

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

3. Arrange $2, 3, 4, \ldots, 21$ in pairs to satify $ab \equiv 1 \pmod{23}$

Look for $23+1=24$, not $2\cdot23+1=47$ (prime), $3\cdot23+1=70$, $4\cdot23+1=93$, $5\cdot23+1=116$, $6\cdot23+1=138$, $7\cdot23+1=162$

$8\cdot23+1=185$, $9\cdot23+1=208$, $10\cdot23+1=231$

$11\cdot23+1=254$, $12\cdot23+1=277$, $13\cdot23+1=300$, $14\cdot23+1=323$

$2 \cdot 12 = 24 \equiv 1 \pmod{23}$
$3 \cdot 8 = 24 \equiv 1$
$4 \cdot 6 = 24 \equiv 1$
$5 \cdot 14 = 70 \equiv 1$
$7 \cdot 10 = 70 \equiv 1$
$9 \cdot 18 = 162 \equiv 1$
$11 \cdot 21 = 231 \equiv 1$
$13 \cdot 16 = 208 \equiv 1$
$15 \cdot 20 = 300 \equiv 1$
$17 \cdot 19 = 323 \equiv 1$

4. Show That $18! \equiv -1 \pmod{437}$

$19 \mid 437$ since $19 \cdot 23 = 437$
By Wilson's Th., $18! \equiv -1 \pmod{19}$
Must show $23 \mid 18! + 1$
By Wilson's Th., $22! \equiv -1 \equiv 22 \pmod{23}$

$\therefore 22!/22 \equiv 22/22 = 1 \pmod{23}$ $\quad$ $\gcd(22, 23) = 1$
$\therefore 21! \equiv 1 \equiv 1 + 23 = 24 \pmod{23}$
$\therefore 21 \cdot 20! \equiv 8 \cdot 3 \pmod{23}$
$\therefore 7 \cdot 20! \equiv 8 \pmod{23}$ $\quad$ $\gcd(3, 23) = 1$
$\therefore 7 \cdot 20 \cdot 19! \equiv 8 \pmod{23}$
$7 \cdot 5 \cdot 19! \equiv 2 \pmod{23}$ $\quad$ $\gcd(4, 23) = 1$
$7 \cdot 5 \cdot 19 \cdot 18! \equiv 2 \pmod{23}$

$\therefore 7 \cdot 5 \cdot 19 \cdot 18! \equiv 2 + 23 = 25 \pmod{23}$

$\therefore 7 \cdot 19 \cdot 18! \equiv 5 \pmod{23}$ $\quad \gcd(5, 23) = 1$

$7 \cdot 19 \cdot 18! \equiv 5 + 23 = 28 \pmod{23}$

$\therefore 19 \cdot 18! \equiv 4 \pmod{23}$ $\quad \gcd(7, 23) = 1$

$19 \cdot 18! \equiv 4 - 23 = -19 \pmod{23}$

$\therefore 18! \equiv -1 \pmod{23}$ $\quad \gcd(19, 23) = 1$

$\therefore 23 \mid 18! + 1$ and $19 \mid 18! + 1$

$\therefore 19 \cdot 23 = 437 \mid 18! + 1$

5. (a) Prove $n > 1$ is prime $\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

Pf: By Wilson's Th and its converse,

n is prime $\Leftrightarrow (n-1)! \equiv -1 \pmod{n}$

$\equiv -1 + n = n - 1 \pmod{n}$

Since $\gcd(n, n-1) = 1$ (prob. #12, sec. 2.2),

$\therefore (n-1)!/(n-1) \equiv (n-1)/(n-1) \pmod{n}$, or

$(n-1)! \equiv -1 \pmod{n} \Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

$\therefore n$ is prime $\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

(b) If n is composite, show $(n-1)! \equiv 0 \pmod{n}$, except when $n = 4$!

Pf: For $n=4$, $(4-1)! = 3! = 6 \equiv 2 \pmod 4$. $\therefore$ Assume $n > 4$.

Since n is composite, let $r \cdot s = n$.

Since $\gcd(n, n-1) = 1$ by prob. #12, sec. 2.2, $1 < r < n-1$. $\therefore$ r must be one of the factor of $(n-1)!$

Similarly, $1 < s < n-1$.

If $r \neq s$, then r and s are different factors in $(n-1)!$, so $n = rs \mid (n-1)!$

$\therefore (n-1)! \equiv 0 \pmod n$

Suppose $r = s$. $\therefore n = r^2$

Now $r < \frac{n}{2}$. For if $r \geq \frac{n}{2}$, then

$n = r^2 \geq \frac{n^2}{4}$, or $4n \geq n^2$, or $4 \geq n$

But $n > 4$, $\therefore r < \frac{n}{2}$

$\therefore 2r < n$, or $2r \leq n-1$

$\therefore$ Both r and $2r \neq r$ are factors of $(n-1)!$

$\therefore r(2r) \mid (n-1)!$, so $r^2 \mid (n-1)!$

$\therefore (n-1)! \equiv 0 \pmod n$

6. Given a prime number p, establish

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

Pf.: From Wilson's Th., $(p-1)! \equiv -1 \equiv -1+p \pmod{p}$

$\therefore p \mid (p-1)! - (p-1)$

Now $1+2+\cdots+n = \frac{n(n+1)}{2}$ for all n.

$\therefore 1+2+\cdots+(p-1) = \frac{(p-1)(p)}{2}$

Since $p-1$ is even, $(p-1)/2$ is an integer, and clearly, $\frac{(p-1)}{2} < p-1$

Also, $(p-1) \mid (p-1)! - (p-1)$

$\therefore \frac{(p-1)}{2} \mid (p-1)! - (p-1)$

Also, $\gcd\left(\frac{p-1}{2}, p\right) = 1$ since p is prime.

$\therefore p$ and $\frac{p-1}{2}$ divide $(p-1)! - (p-1)$, so

$p\frac{(p-1)}{2} = 1+2+\cdots+(p-1)$ divides $(p-1)! - (p-1)$

$\therefore (p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}$

7. If p is prime, prove that for any a,

$p \mid a^p + (p-1)!\,a$ and $p \mid (p-1)!\,a^p + a$

(a) $p \mid a^p + (p-1)!a$

Pf: By corollary to Fermat's Th, $a^p \equiv a \pmod p$, for any a.

By Wilson's Th., $-1 \equiv (p-1)! \pmod p$

$\therefore$ By multiplying, $-a^p \equiv (p-1)!a \pmod p$,

or, $a^p \equiv -(p-1)!a \pmod p$

$\therefore p \mid a^p + (p-1)!a$

(b) $p \mid (p-1)!a^p + a$

Pf: As in (a), $(p-1)! \equiv -1 \pmod p$

$a^p \equiv a \pmod p$

Multiplying together, $a^p(p-1)! \equiv -a \pmod p$, or

$p \mid a^p(p-1)! + a$

8. Find two odd primes $p \leq 13$ s.t. $(p-1)! \equiv -1 \pmod{p^2}$

5: $4! + 1 = 25$, so $p^2 \mid (p-1)! + 1$

7: $6!+1 = 721$, $7^2 \nmid 721$

9: $8!+1 = 40321$, $9 \nmid 40321$

11: $10!+1 = 3{,}628{,}801$, $11^2 \nmid 3{,}628{,}801$

13: $12!+1 = 479{,}001{,}601$, and $13^2 \mid 479{,}001{,}601$

9. Prove for any odd prime, $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$

Pf: $K \equiv K-p = -(p-K) \pmod p$

$$\therefore \left.\begin{aligned} 2 &\equiv -(p-2) \pmod p \\ 4 &\equiv -(p-4) \pmod p \\ &\vdots \\ p-1 &\equiv -1 \pmod p \end{aligned}\right\} \frac{p-1}{2} \text{ factors } (p>2)$$

$\therefore 2 \cdot 4 \cdots (p-1) \equiv (-1)(-3) \cdots [-(p-2)] \pmod p$, $p > 2$

There are $(p-1)/2$ factors, so

$$2 \cdot 4 \cdots (p-1) \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdots (p-2) \pmod p$$

Now, multiply both sides by $1 \cdot 3 \cdot 5 \cdots (p-2)$

$\therefore 1\cdot 2\cdot 3\cdot 4\cdots(p-2)(p-1) = (p-1)! \equiv (-1)^{\frac{p-1}{2}} 1^2\cdot 3^2\cdots(p-2)^2 \pmod{p}$

Or, $(p-1)! \equiv (-1)^{\frac{p-1}{2}} 1^2\cdot 3^2\cdots(p-2)^2 \pmod{p}$

By Wilson's Th., $-1 \equiv (p-1)! \pmod{p}$

$\therefore\ -1 \equiv (-1)^{\frac{p-1}{2}} 1^2\cdot 3^2\cdots(p-2)^2 \pmod{p}$

Multiplying both sides by $(-1)^{\frac{p-1}{2}}$, and noting that $\left[(-1)^{\frac{p-1}{2}}\right]^2 = 1$ since $(-1)^{\frac{p-1}{2}} = 1$ or -1, and noting $-1 = (-1)^{\frac{2}{2}}$,

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

$\therefore\ (-1)^{\frac{p+1}{2}} \equiv 1^2\cdot 3^2\cdots(p-2)^2 \pmod{p}$

10. (a) For a prime p of the form $4k+3$, prove either

$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p}$ or $\left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$

Pf: If p is any prime, $ab \equiv 0 \pmod{p} \Rightarrow$ $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$ (see end of

Section 4.2, proved a beginning of solutions to problems of 4.2, labelled Theorem 2).

$\therefore$ If a is any integer, $a^2 \equiv 1 \pmod{p} \Rightarrow$
$a^2 - 1 \equiv 0 \pmod{p}$, $\therefore$ $a+1 \equiv 0 \pmod{p}$ or
$a - 1 \equiv 0 \pmod{p}$
$\therefore$ $a^2 \equiv 1 \pmod{p} \Rightarrow a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$

In the proof to Theorem 5.5 on p. 100,

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

Multiplying both sides by $(-1)^{\frac{p-1}{2}}$ and

noting $(-1) = (-1)^{\frac{2}{2}}$,

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

Now, if p is of the form $4k+3$, then

$$(-1)^{\frac{4k+4}{2}} = (-1)^{2k+2} = 1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

$\therefore$ From above, $\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p}$, or

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

(6) if $p = 4k+3$ is prime, then the product of all the even integers $< p$ is congruent mod p to either 1 or -1.

Pf: Let $2, 4, 6, \ldots, a$ be all even integers $< p$

$\therefore a = p-1$.

Consider $2 \cdot 4 \cdot 6 \cdot \cdots \cdot a = 2^k (1 \cdot 2 \cdot 3 \cdots \frac{a}{2})$,

where $k = \#$ of terms in $2, 4, 6, \ldots, a$

Since $a/2 = (p-1)/2$, then $k = (p-1)/2$

$\therefore 2 \cdot 4 \cdot 6 \cdots a = 2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)\right)$

$= 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$ [1]

By Fermat's Th., $2^{p-1} \equiv 1 \pmod{p}$, since $p \nmid 2$ as p is an odd prime.

$\therefore 2^{p-1} = \left(2^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$, so

$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

Multiplying both sides by $\left(\frac{p-1}{2}\right)!$,

$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p}$ or $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$

$\therefore$ From [1] above,

$2\cdot 4\cdot 6 \cdots a \equiv 1 \pmod{p}$ or $2\cdot 4\cdot 6 \cdots a \equiv (-1) \pmod{p}$

Note: above just used p as an odd prime. Could be of $4k+1$ form as well.

11. Obtain two solutions to $x^2 \equiv -1 \pmod{29}$ and $x^2 \equiv -1 \pmod{37}$

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

As, $29 \equiv 1 \pmod{4}$, there is a solution, and the proof of Th. 5.5 shows that

$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1) \pmod{p}$. $\therefore \pm\left(\frac{29-1}{2}\right)! = \pm 14!$

$\therefore 14!$ or $-14!$ is a solution

(b) $x^2 \equiv -1 \pmod{37}$. As $37 \equiv 1 \pmod{4}$, as in (a),
$\left(\frac{37-1}{2}\right)! = 18!$ $\therefore 18!$ or $-18!$ is a solution.

12. Show that if $p = 4k+3$ is prime and $a^2+b^2 \equiv 0 \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$

Pf: Suppose $a \not\equiv 0 \pmod{p}$. $\therefore p \nmid a$

Consider $ax \equiv 1 \pmod{p}$. By Th. 4.7, there is a unique solution mod p, and so there is a unique integer c s.t. $1 \le c \le p-1$ and $ac \equiv 1 \pmod{p}$. $\therefore a^2c^2 \equiv 1 \pmod{p}$

From $a^2 + b^2 \equiv 0 \pmod{p}$, after multiplying both sides by c^2, you get

$a^2c^2 + b^2c^2 \equiv 0 \pmod{p}$. But $a^2c^2 \equiv 1 \pmod{p}$

$\therefore 1 + b^2c^2 \equiv 0 \pmod{p}$

$\therefore x = bc$ is a solution to $x^2 + 1 \equiv 0 \pmod{p}$, which, by Th. 5.5, means $p \equiv 1 \pmod{4}$. But this contradicts $p = 4k+3 \Rightarrow p \equiv 3 \pmod{4}$

$\therefore a \equiv 0 \pmod{p}$

The exact same reasoning applies to b, so that $b \equiv 0 \pmod{p}$.

13. Supply details in the proof that $\sqrt{2}$ is irrational.

Pf: Suppose $\sqrt{2} = a/b$, $\gcd(a,b) = 1$

Then $a^2 = 2b^2$

$\therefore a^2 + b^2 = 3b^2$, and $\therefore 3 \mid (a^2+b^2)$, or
$a^2+b^2 \equiv 0 \pmod 3$

$\therefore$ From problem # 12 above, since 3 is a prime of form $p = 4k+3$, Then
$a \equiv b \equiv 0 \pmod 3$
$\therefore 3 \mid a$ and $3 \mid b$, contradicting $\gcd(a,b) = 1$.

14. Prove the odd prime divisors of n^2+1 are of the form $4k+1$.

Pf: Let p be an odd prime divisor of n^2+1

$\therefore n^2 + 1 \equiv 0 \pmod p$

$\therefore n$ is a solution to $x^2+1 \equiv 0 \pmod p$, and by Th. 5.5, p is of form $4k+1$

15. Verify $4(29!) + 5!$ is divisible by 31.

By Wilson's Th., $30! \equiv -1 \pmod{31}$

$\therefore\ 30 \cdot 29! \equiv 31 - 1 = 30 \pmod{31}$

$\therefore\ 29! \equiv 1 \pmod{31}$ as $\gcd(30, 31) = 1$

$\therefore\ 4(29!) \equiv 4 \pmod{31}$

$5! = 120 \quad \therefore\ 4(29!) + 5! \equiv 4 + 120 = 124 \pmod{31}$

But $124 = 4 \cdot 31$

$\therefore\ 4(29!) + 5! \equiv 0 \pmod{31}$

$$\Rightarrow 31 \mid (4(29!) + 5!)$$

16. For a prime p and $0 \le k \le p-1$, show that

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

Pf: $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots (p-k-1)(p-k) \cdots (p-2)(p-1)$

$= (p-k-1)!\,(p-k) \cdots (p-2)(p-1)$

But $p-1 \equiv -1 \pmod{p}$

$p-2 \equiv -2 \pmod{p}$

$\vdots$

$p-k \equiv -k \pmod{p}$

$\therefore\ (p-k) \cdots (p-2)(p-1) \equiv (-k) \cdots (-2)(-1) \pmod{p}$

But $(-k) \cdots (-2)(-1) = (-1)^k k!$

$\therefore (p-k)\cdots(p-2)(p-1) \equiv (-1)^k k! \pmod p$

$\therefore (p-k-1)!\,(p-k)\cdots(p-2)(p-1) \equiv (-1)^k k!\,(p-k-1)! \pmod p$

$\therefore (p-1)! \equiv (-1)^k k!\,(p-k-1)! \pmod p$

By Wilson's Th., $(p-1)! \equiv -1 \pmod p$

$\therefore (-1) \equiv (-1)^k k!\,(p-k-1)! \pmod p$ [1]

Since $(-1)^k \cdot (-1)^k = 1$, and $(-1)(-1)^k = (-1)^{k+1}$, after multiplying both sides of [1] by $(-1)^k$, you get

$$(-1)^{k+1} \equiv k!\,(p-k-1)! \pmod p$$

17. If p, q are distinct primes, prove for any integer a,

$$pq \mid a^{pq} - a^p - a^q + a$$

Pf: Consider $(a^p)^q - a^p$. By the corollary to Fermat's Th., $x^q \equiv x \pmod q$, so letting $x = a^p$, $q \mid (a^p)^q - a^p$. Also $a^q \equiv a \pmod q$. $\therefore q \mid a^q - a$.

$$\therefore q \mid [(a^p)^q - a^p] - (a^q - a) = a^{pq} - a^p - a^q + a$$

Similarly, $p \mid (a^q)^p - a^q$ and $p \mid a^p - a$

$\therefore \; p \mid [(a^q)^p - a^q] - (a^p - a) = a^{pq} - a^p - a^q + a$

$\therefore$ Both p and q divide $a^{pq} - a^p - a^q + a$, and so by corollary 2, sec. 2.2,

$pq \mid a^{pq} - a^p - a^q + a$

18. Prove if p and $p+2$ are twin primes, then

$$4\left((p-1)! + 1\right) + p \equiv 0 \pmod{p(p+2)}$$

Pf: $(p-1)! \equiv -1 \pmod{p}$ Wilson's Th.

$\therefore \; (p-1)! + 1 \equiv 0 \pmod{p}$

$\therefore \; 4[(p-1)! + 1] \equiv 0 \pmod{p}$

$\therefore \; 4[(p-1)! + 1] + p \equiv 0 \pmod{p}$ [1]

Also, $(p+2-1)! = (p+1)! \equiv -1 \pmod{p+2}$ Wilson's Th.

$\therefore \; (p+1)p! \equiv -1 + p + 2 = p+1 \pmod{p+2}$

$\therefore p! \equiv 1 \pmod{(p+2)}$ as $\gcd(p+1, p+2) = 1$

$\therefore 4p! \equiv 4 = 4 + 2p - 2p = 2(p+2) - 2p \pmod{(p+2)}$

$\therefore 4p\,(p-1)! \equiv -2p \pmod{(p+2)}$

$\therefore 4\,(p-1)! \equiv -2 \pmod{(p+2)}$ $\qquad \gcd(p, p+2) = 1$

$\therefore 4\,(p-1)! + p + 2 \equiv -2 \pmod{(p+2)}$

$\therefore 4\,(p-1)! + p + 4 \equiv 0 \pmod{(p+2)}$

$\therefore 4\,[(p-1)! + 1] + p \equiv 0 \pmod{(p+2)}$ $\qquad [2]$

$\therefore$ p and $p+2$ divide $4\,[(p-1)! + 1] + p$ by [1], [2]

$\therefore$ $p(p+2)$ divides $4\,[(p-1)! + 1] + p$ by corollary 2, section 2.2.

$\therefore 4\,[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}$