1. Wilson's Theorem

Theorem. Let $p > 2$ be a prime number, then $(p-2)! \equiv 1, (p-1)! \equiv -1 \pmod{p}$.

Proof: The result is true for p=2, 3, and 5. So assume p>5, and let's take a closer look at the mod p values of 1, 2, 3, ..., p-2, and p-1.

$1 \equiv 1^{-1}, p-1 \equiv -1 \equiv (p-1)^{-1} \ (mod\ p)$, which means 1 and p-1 are their own inverse.

For $S = \{2,3,4, \dots, p-2\}$, there are p-3 (which is even) numbers. For each $s \in S, s^{-1} \in S$. And $s \neq s^{-1}$, for otherwise we have $s^2 \equiv 1\ (mod\ p), \Rightarrow p|(s-1)(s+1)$, which is impossible for $s \in S = \{2,3,4, \dots, p-2\}$.

Thus we can group the p-3 numbers of S as $\frac{p-3}{2}$ pairs, each pair is in form of $s \cdot s^{-1} \equiv 1\ (mod\ p)$. Thus $2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) \equiv 1\ (mod\ p)$.

Combined S with 1 and p-1, we have $(p-2)! \equiv 1$, and $(p-1)! \equiv -1$.

Note: The only two numbers in $\{1,2, \dots, p-1\}$ which have their inverse equal to themselves, are 1 and p-1. Because $p|a^2 - 1 \Rightarrow\ a \equiv \pm 1$ (mod p).

Theorem. Converse of Wilson. If n>2 and $(n-1)! \equiv -1\ (mod\ n)$, then n is a prime number.
Proof: For otherwise if n has a divisor d, $d|n, d \leq n-2$, thus $d|(n-1)!$. Since $n|(n-1)! + 1$, and d|n, this leads to d|1. Thus n must be a prime.

1). Prove there are infinitely many composite numbers of form n!+1.

Solution: Let p>2 be a prime, then $p|(p-1)! + 1$, so $(p-1)! + 1$ is a composite number. Since there are infinitely many prime numbers, and each $(p-1)! + 1$ is composite, we are done.

2). Find the following remainders:

a). 15! divided by 17.

b). 2*26! divided by 29.

c). 4*29!+5! divided by 31.

Solution: a). 1

b). $26! \cdot 27 \equiv 1\ \Rightarrow 26! \cdot (-2) \equiv 1\ \Rightarrow 26! \cdot 2 \equiv -1$ (mod 29)

c). $4 * 29! + 5! \equiv 4 * 1 + 120 \equiv 124 \equiv 0\ \ (mod\ 31)$

3). Prove: $18! \equiv -1 \pmod{437}$.

Solution: 437=19*23. $18! \equiv -1 \ (mod\ 19)$.
$18! \cdot 19 \cdot 20 \cdot 21 \equiv 1 \ (mod\ 23)$, thus $18! \cdot (-4) \cdot (-3) \cdot (-2) \equiv 1$,
$\Rightarrow\ 18! \cdot (-24) \equiv 1\ \ \Rightarrow 18! \cdot (-1) \equiv 1\ \ \Rightarrow 18! \equiv -1\ \ (mod\ 23)$.

Thus $18! \equiv -1\ (mod\ 437 = 19 * 23)$.

4). Property. If n>4 is a composite number, then $(n-1)! \equiv 0\ \ (mod\ n)$.

Solution: Since n is composite, then $n = d * m$ for some divisors where both d and m are within 2 to n-1 range. If $d \neq m$ then they both appear in (n-1)!.

If d=m is the only way to factor n=d*m, then $n = p^2$ for d=m=p, $p > 2$, thus p and 2p both appear in (n-1)!. Thus $(n-1)! \equiv 0\ \ (mod\ p^2)$

5). P is a prime number, show $(p-1)! \equiv p-1\ \ \ (mod\ 1+2+3+\cdots+(p-1))$

Solution: $1+2+3+\cdots+(p-1) = p\frac{p-1}{2}$. p and $\frac{p-1}{2}$ are co-prime, and $(p-1)! \equiv p - 1\ (mod\ p)$, $(p-1)! \equiv 0\ \ \left(mod\ \frac{p-1}{2}\right)$. We see p-1 satisfy both conditions. By the Chinese remainder theorem, p-1 is the only solution.

6). Lemma. If p is an odd prime number, prove: $1^2 \cdot 3^2 \cdot 5^2 \ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}}\ \ (mod\ p)$

Solution: $(p-1)(p-3)\ldots 6 \cdot 4 \cdot 2 \equiv (-1)(-3)\ldots\big(-(p-6)\big)\big(-(p-4)\big)\big(-(p-2)\big)$. Thus
$1^2 \cdot 3^2 \cdot 5^2 \ldots (p-2)^2 \equiv [1 \cdot 3 \cdot 5 \ldots (p-2)] \cdot \left[(p-1)(p-3)\ldots 6 \cdot 4 \cdot 2 \cdot (-1)^{\frac{p-1}{2}}\right]$
$\equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv (-1)^{\frac{p+1}{2}}\ \ \ (mod\ p)$

7). Lemma. If p is a prime of form 4k+3, prove $\left(\frac{p-1}{2}\right)! \equiv \pm 1\ \ (mod\ p)$, hence $\left(\frac{p-1}{2}\right)!$ is a solution to the equation $x^2 \equiv 1\ \ (mod\ p)$.

Solution: The numbers from 1 to p-1 can be arranged as the first half, and the 2nd half:
$1,2,3,\ldots,\dfrac{p-1}{2},\qquad \dfrac{p+1}{2},\dfrac{p+3}{2},\ldots,p-1$
The 2nd half is indeed the "modulo negatives" of the first half:
$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -2, -1$, Combining the two halves, we have:
$-1 \equiv (p-1)! \equiv \left(\dfrac{p-1}{2}\right)!\left(\dfrac{p-1}{2}\right)!\,(-1)^{\frac{p-1}{2}}$

$$\Rightarrow\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv(-1)^{\frac{p+1}{2}}\equiv(-1)^{2k+2}\equiv 1\ (mod\ p)\ \Rightarrow p\left|\left(\left(\frac{p-1}{2}\right)!-1\right)\left(\left(\frac{p-1}{2}\right)!+1\right)\right.$$

8). Lemma. If p is prime of form 4k+1, prove $\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv -1\ \ (mod\ p)$, hence $\left(\frac{p-1}{2}\right)!$ is a solution to the equation $x^2+1\equiv 0\ \ (mod\ p)$.

9). Compute $(6!)^2$ (mod 13), $(9!)^2$ mod (19)

Solution: p=13 is 4k+1, $(6!)^2\equiv -1\equiv 12\ \ (mod\ 13)$.

p=19 is 4k+3, $(9!)^2\equiv 1\ \ (mod\ 19)$.

10). For prime p, and $0\le k\le p-1$, prove $k!\,(p-1-k)!\equiv(-1)^{k+1}\ \ (mod\ p)$

Solution: $1\cdot 2\cdot\ldots\cdot k\equiv(-1)^k(p-1)(p-2)\ldots(p-k)$, thus we have

$k!\,(p-1-k)!\equiv(-1)^k(p-1)(p-2)\ldots(p-k)(p-1-k)!\equiv(-1)^k(p-1)!$

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

11). If p and p+2 are a pair of twin primes, then $4\big((p-1)!+1\big)+p\equiv 0\ \ \ (mod\ p(p+2))$

Solution: Under modulo p, $4\big((p-1)!+1\big)+p\equiv 4(-1+1)+p\equiv 0$.

Under modulo p+2, $4\big((p-1)!+1\big)+p\equiv 4(p-1)!+p+4\equiv -2(-2)(p-1)!+2$
$\equiv -2(p)(p-1)!+2\equiv -2*p!+2\equiv 0$
Since p and p+2 are co-prime, hence $4\big((p-1)!+1\big)+p\equiv 0\ \ \ (mod\ p(p+2))$.

12). Find the remainder when 2014! is divided by 2017.

Solution: Notice 2017 is a prime number. Thus $2014!\equiv 2015^{-1}\equiv -(2^{-1})$ (mod 2017)

Since $2^{-1}\equiv\frac{2018}{2}\equiv 1009$, thus $-(2^{-1})\equiv -1009=1008$.

13). Let a be an integer such that $\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{23}=\frac{a}{23!}$. Find the remainder when a is divided by 13.

Solution: If we make the common denominator for the LHS as 23!, the numerator from each component will be a multiple of 13, except the number from 1/13.

The numerator from 1/13 is $1\cdot 2\cdot\ldots\cdot 12\cdot 14\cdot 15\cdot\ldots\cdot 23\equiv 12!*10!\equiv(-1)*1*$
$11^{-1}\ \ (mod\ 13)$. Since $11*6\equiv 1\ \ (mod\ 13)$, the answer is $-6\equiv 7$ (mod 13).

14). Lemma. For odd prime p, $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv p+(p-1)! \pmod{p^2}$.

Proof: Per Fermat, $k^{p-1}\equiv 1$ (mod p), but it is harder for mod p^2. We proceed carefully:

Let $k^{p-1}=a_k p+1$, $(p-1)!^{p-1}\equiv(a_1p+1)(a_2p+1)\ldots(a_{p-1}p+1)$

$\equiv 1+(a_1+a_2+\cdots+a_{p-1})p \pmod{p^2}$.

From Wilson, $(p-1)!=kp-1$, thus

$(p-1)!^{p-1}=(kp-1)^{p-1}\equiv(-1)^{p-1}+(-1)^{p-2}(p-1)pk\equiv 1+pk \pmod{p^2}$.

This means $(a_1+a_2+\cdots+a_{p-1})p\equiv pk=(p-1)!+1 \pmod{p^2}$.

We have now: $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}=(a_1p+1)+(a_2p+1)+\cdots+(a_{p-1}p+1)$

$=p-1+(a_1+a_2+\cdots+a_{p-1})p\equiv p-1+(p-1)!+1=p+(p-1)! \pmod{p^2}$.

15). Find positive integer n and m such that $(n-1)!+1=n^m$.

Solution: We need $n|(n-1)!+1$, thus n must be a prime number.

First of all, (n, m)=(2, 1), (3, 1), and (5, 2) works. We show n>5 is impossible.

$(n-1)!=(n-2)!\,(n-1)=n^m-1\ \Rightarrow\ (n-2)!=n^{m-1}+n^{m-2}+\cdots+n+1$

If we take mod n-1, this gives $(n-2)!\equiv m$ (mod n-1).

Notice for all prime n>5, n-1 is composite, thus $n-1|(n-2)!$, so $m=k(n-1)$, $k\geq 1$.

$(n-1)!+1=n^m\geq n^{(n-1)}$, that is impossible.

16). Is it possible that $a_1,a_2,\ldots,a_n$ as a permutation of {1, 2, ..., n}, such that $\{a_1,a_1a_2,$ $a_1a_2a_3,\ldots,a_1a_1\ldots a_n\}$ is a complete residue class mod n?

Solution: If $a_i=n, i<n$, then $a_1a_1\ldots a_i\equiv a_1a_1\ldots a_n\equiv 0$ (mod n), thus n must be a_n.

Then $a_1a_1\ldots a_{n-1}=(n-1)!$, and it is NOT a multiple of n, so either n<5 or n is a prime.

For n=4, we see $a_1=1, a_2=3, a_3=2, a_4=4$ works.

Any for any prime number $n\geq 5$, for example if we could have $a_1a_2\ldots a_i\equiv i$ (mod n), this would fit Wilson: $a_1a_1\ldots a_{n-1}\equiv(n-1)!\equiv -1$. Thus we need:

$$a_1a_2\ldots a_i=a_1a_2\ldots a_{i-1}\cdot a_i\equiv(i-1)\cdot a_i\equiv i\Rightarrow\ a_i\equiv\frac{i}{i-1}\equiv 1+(i-1)^{-1}$$

Hence define $a_1=1, a_i\equiv 1+(i-1)^{-1}, a_n=n$, we are done.

2. Fermat's Little Theorem

Theorem. If p is a prime number and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.

Proof: $p \nmid a$ means a and p are coprime. Now consider the following $p-1$ numbers:

$a, 2a, 3a, \dots, (p-1)a$.

This is a complete residue class of mod p, excluding 0, so their product should equal $(p-1)!$ when taking mod p, hence we have:

$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p$

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

Corollary: If p is a prime number and a is any integer, then $a^p \equiv a \pmod p$

Another proof: We apply proof by induction. Suppose $a^p \equiv a \pmod p$ for integer a, now we aim to show $(a+1)^p \equiv a+1 \pmod p$.

Consider the binomial expansion of $(a+1)^p$:

$$(a+1)^p = a^p + \binom{p}{p-1} a^{p-1} + \binom{p}{p-2} a^{p-2} + \dots + \binom{p}{1} a^1 + 1$$

$\binom{p}{p-k} a^{p-k} \equiv 0 \pmod p, k = 1, 2, \dots, p-1$, because $p \mid \binom{p}{p-k}$

$\Rightarrow (a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$

Example: $3^{31} \equiv 3^{30} \cdot 3 \equiv (3^6)^5 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod 7$

Compute $29^{25} \pmod{11}$

Solution: $29^{25} \equiv 7^{25} \equiv 7^5 \equiv 10 \pmod{11}$

Compute $128^{129} \pmod{17}$

Solution: $128^{129} \equiv 9^{129} \equiv 9^{128} \cdot 9 \equiv 9 \pmod{17}$

Note: The converse of Fermat theorem is not true. That is, if $a^{n-1} \equiv 1 \pmod n$, n does not always need to be a prime number.

Theorem. If p is an odd prime, and there exist integer x such that $x^2 \equiv -1 \pmod p$, then $p \equiv 1 \pmod 4$.

Proof: First of all, all odd primes p are either 1 or 3 when mod 4.

If $x^2 \equiv -1$, then $x^4 \equiv 1$, thus $x^{4k} \equiv 1$. Now from Fermat, $x^{p-1} \equiv 1$, in case $p = 4k+3$, then

$x^{p-1} \equiv x^{4k+2} \equiv x^2 \equiv -1$, a contradiction!

On the other hand we see if $p = 4k+1$, then $x^{p-1} \equiv x^{4k} \equiv 1$, all is good.

Note: $x^2 \equiv -1 \pmod p \iff x^2 + 1 \equiv 0 \pmod p$.

Theorem. If prime number p is of form $4k+1$, then $x^2 + 1 \equiv 0 \pmod p$ has integer solution.

Proof: Let $p = 4k+1$, we aim to find a solution for $x^2 + 1 \equiv 0 \pmod p$.

But in the Wilson's Theorem section, we already showed that $\left(\frac{p-1}{2}\right)!$ is a solution to the equation $x^2 + 1 \equiv 0 \pmod p$.

For example, p=13 is such a prime, $\left(\frac{p-1}{2}\right)! = 6! = 720 \equiv 5 \ (mod\ 13)$, and $5^2 + 1 \equiv 0 \pmod{13}$.

Summary:

$$p = 4k+1 \iff \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \iff x^2 + 1 \equiv 0 \pmod p \text{ has solution}$$

$$p = 4k+3 \iff \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \ (mod\ p)$$

Note: $x^2 - 1 \equiv 0 \pmod p$ is a trivial equation since $x^2 - 1 = (x-1)(x+1)$ thus 1 and $p-1$ are always solutions to this equation. So $x^2 - 1 \equiv 0 \pmod p$ does not lead to any conclusion on p itself. In comparison, $x^2 + 1 \equiv 0 \pmod p$ is special, if it has a solution, then p must be $4k+1$.

Theorem: All the odd prime factors of $n^2 + 1$ must be in form of $4k+1$.

Proof: Suppose p is odd and $p | n^2 + 1$. This means $n^2 + 1 \equiv 0 \pmod p$. The result follows.

Think: What about the odd prime factors of $n^2 - 1$? Do they have to be in form of $4k+3$?

Answer is no. $n^2 - 1 \equiv 0\ (mod\ p)$ always have solution 1 and p-1 and thus does not lead to any indication on p. In fact, $n^{p-1} \equiv n^{4k+2}\ or\ n^{4k}$, both cases will always be 1 mod p.

Theorem. If a and b are co-prime positive integers, then every prime divisor of $a^2 + b^2$ is either 2 or of form $4k + 1$.
Proof: If a and b are both odd than p can be 2.
Suppose p is an odd prime, then since a and b are co-prime, at least one of them is not a multiple of p. Suppose $p \nmid a$, so a^{-1} exists.
$a^2 + b^2 \equiv 0$, multiply a^{-2} we get $b^2 + 1 \equiv 0$ (mod p), from the previous theorem, p must be 4k+1 form.

Theorem. If p is a prime of form $4k + 3$, and $a^2 + b^2 \equiv 0\ \ (mod\ p)$, then $a \equiv b \equiv 0\ (mod\ p)$.

Solution: Suppose otherwise, a is co-prime to p, then there exists a mod-p inverse for a:
$ac \equiv 1\ (mod\ p),\ \Rightarrow a^2c^2 \equiv 1, b^2c^2 \equiv -1\ (mod\ p)$.

So now bc is a solution to equation $x^2 + 1 \equiv 0$, P must be of form 4k+1, a contradiction.

Note: A common technique to prove $p \nmid a$, is to assume otherwise a has modular inverse.

Corollary: **Fermat's Christmas theorem**: A prime number p can be represented as a sum of two non-zero squares, if and only if $p = 2$ or $p \equiv 1\ (mod\ 4)$.

Lemma. Let p be a prime, and **n is co-prime to $\boldsymbol{p - 1}$**, then $1^n, 2^n, \dots, (p-1)^n$ form a reduced set of residues mod p.

Proof: All we need to show is $i^n \not\equiv j^n$, for $1 \le i < j \le p - 1$.

For otherwise, $i^n \equiv j^n$, and $i^{p-1} \equiv j^{p-1} \equiv 1$ (mod p), thus $i^{\gcd(p-1,n)} \equiv j^{\gcd(p-1,n)}$,

Which means $i \equiv j$, contradiction.

Corollary. Let p be a prime, and n is co-prime to $p - 1$, then$1^n + 2^n + \cdots + (p-1)^n \equiv 0$.

For odd prime p, if $n = 2$ in the above lemma, we get:

$1^2 + 2^2 + \cdots + (p-1)^2 \equiv 0\ $ (mod p)

For prime p>3, $n = 3$ in the above lemma, we get:

$1^3 + 2^3 + \cdots + (p-1)^3 \equiv 0\ $ (mod p)

- **3k+1 vs 3k+2**

Similar to 4k+1 vs 4k+3, there is a lot to say about a prime in form of 3k+1 or 3k+2.

Lemma. If p is a prime of form 3k+2, then $1^3, 2^3, \dots, (p-1)^3$ is a reduced set of residues mod p.

This come directly from the lemma, that if n is co-prime to $p-1$, then $1^n, 2^n, \dots, (p-1)^n$ form a reduced set of residues mod p.

This lemma can mean a lot, for example it leads to the following:

Lemma. If p is a prime of form 3k+2, and $a^2+ab+b^2 \equiv 0 \pmod{p}$, then $p|a, and\ p|b$.

Proof: If p|a, then p|b. So assume $p \nmid ab$, from $a^3 \equiv b^3$ (mod p), since $1^3, 2^3, \dots, (p-1)^3$ are each distinct mod p, thus $a \equiv b$ (mod p), $a^2+ab+b^2 \equiv 3a^2 \equiv 0$, contradiction.

Corollary. If p is a prime of form 3k+2, then $x^2+x+1 \equiv 0 \pmod{p}$ has no solution.

Theorem. All prime divisors of n^2+n+1 must be of form 3k+1.

Note: Compare this to: All the odd prime factors of n^2+1 must be in form of $4k+1$.

Example. Is there integer x such that $x^2 \equiv -3$ (mod 101)?
Solution: 101 is a prime of form 3k+2. Suppose $x^2+3 \equiv 0$, mod 101.
Notice $x \equiv 2y+1$ has solution for y, this means $4y^2+4y+4 \equiv 0$, $y^2+y+1 \equiv 0$, contradiction.

Property. If p is a prime of form 3k+2, then $x^2 \equiv -3$ (mod p) has no solution.
More on this when we study Quadratic Residues.

Note: For any $1 \le a < b \le p-1$, we have:

$a^3 \equiv b^3 \iff a^2+ab+b^2 \equiv 0$ (mod p).

Multiply by b^{-2}, we get $(a/b)^2+(a/b)+1 \equiv 0$, let $2(a/b)+1 = c$, then

$a^3 \equiv b^3 \iff c^2 \equiv -3$ has solution in mod p.

Lemma. If p is a prime of form 3k+1, then $1^3, 2^3, \dots, (p-1)^3$ is NOT a reduced set of residues mod p.

Proof: If r is a primitive root mod p, and $r \equiv x^3$, then $r^k \equiv x^{3k} \equiv 1$ (mod p), this contradicts the fact that r is a primitive root.

Note: We will revisit this when we study primitive root.

Example. There are infinitely many primes numbers of form 6k+1.
Proof: Suppose there are only finite, $p_1, p_2, \ldots, p_N$, now consider:
$(p_1p_2 \ \ldots p_N)^2 + (p_1p_2 \ \ldots p_N) + 1$, its prime factor must be of form 3k+1, but it is not divisible by any of the p_i we have in the list.
Notice any odd prime of 3k+1 must be of form 6k+1.

3. More Examples

1). Prove $a^5 \equiv a \ \ (mod\ 10)$

Solution: $a^5 \equiv a \ \ (mod\ 5)$, and $a^5 \equiv a \ \ (mod\ 2)$.

Note: This shows the a^5 has the same units digit as a.

2). If a is not a multiple of 7, then either $a^3 + 1$ or $a^3 - 1$ is a multiple of 7.

Solution: $a^6 \equiv 1 \ \ (mod\ 7)$, this means $7|a^6 - 1 = (a^3 + 1)(a^3 - 1)$. This gives way to the following result:

3). Lemma. Let p be an odd prime, and $p \nmid a$, prove $a^{\frac{p-1}{2}}$ (mod p) is either 1 or -1.

Solution: $p|a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, so p divides either $a^{\frac{p-1}{2}} - 1$ or $a^{\frac{p-1}{2}} + 1$.

4). Lemma. p is a prime number, $p \nmid a, \ p \nmid b$. If $a^p \equiv b^p \ (mod\ p)$, then $a^p \equiv b^p \ \ (mod\ p^2)$

Solution: $a^{p-1} \equiv 1 \equiv b^{p-1} \ (mod\ p) \ \Rightarrow a \equiv b \ \ (mod\ p)$. $a = b + kp$ for some integer k.

$$a^p - b^p = (b + kp)^p - b^p = \binom{p}{p-1} b^{p-1}kp + \cdots + \binom{p}{1} b(kp)^{p-1} + (kp)^p$$

Notice in the sum, the first term is divisible by p^2, all other terms have higher powers of p.

5). If p is a odd prime number, prove:

(a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \ \ (mod\ p)$

(b) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \ \ (mod\ p)$

Solution: (a) is direct from Fermat. For (b), notice

$$1+2+3+\cdots+(p-1)=\frac{p}{2}(p-1)\equiv 0\ (mod\ p)$$

6). Lemma. If p is a odd prime number, and $1\leq k\leq p-1$, prove:

$$\binom{p-1}{k}\equiv(-1)^k\ \ (mod\ p)$$

Solution: $(p-1)(p-2)\ldots(p-k)\equiv(-1)(-2)\ldots(-k)\equiv(-1)^k k!\ \ (mod\ p)$, dividing this by k! on both sides we get the result. (We can divide by k! since it is co-prime to p).

$$\binom{p-1}{k}=\frac{(p-1)(p-2)\ldots(p-k)}{k!}\equiv(-1)^k\ \ (mod\ p)$$

Corollary. For all $1\leq k\leq p-1$, we have: $k!\,(p-k-1)!+(-1)^k\equiv 0$ (mod p).

$$\binom{p-1}{k}=\frac{(p-1)!}{k!\,(p-k-1)!}\equiv(-1)^k\ \Rightarrow\ k!\,(p-k-1)!\equiv(-1)^k(p-1)!\ \ (mod\ p)$$

$$\Rightarrow\ k!\,(p-k-1)!\equiv(-1)^{k+1}\ (\text{mod p})$$

7). Lemma. If p and q are odd prime numbers such that $p-1|q-1$, and a is not a multiple of p or q, prove that $a^{q-1}\equiv 1\ \ (mod\ pq)$.

Solution: $a^{q-1}\equiv 1\ (mod\ q)$, $a^{p-1}\equiv 1\ (mod\ p)\Rightarrow\ p|a^{p-1}-1\ |a^{q-1}-1$.

Thus $a^{q-1}\equiv 1\ \ (mod\ pq)$.

For example, p=3, q=7, then $a^6\equiv 1\ \ (mod\ 21)$ as long as a is not a multiple of 3 or 7.

8). P and q are distinct prime numbers, prove: $p^{q-1}+q^{p-1}\equiv 1\ \ (mod\ pq)$

Solution: $p^{q-1}+q^{p-1}\equiv 1+0\equiv 1\ \ (mod\ q)$, $p^{q-1}+q^{p-1}\equiv 0+1\equiv 1\ \ (mod\ p)$.

9). Property. P is an odd prime, prove $a^{2p-1}\equiv a\ (mod\ 2p)$ for any integer a.

Solution: $a^{2p-1}\equiv a\ (mod\ 2)$. $a^{2p-1}\equiv a^p\cdot a^{p-1}\equiv a\cdot a^{p-1}\equiv a^p\equiv a\ (mod\ p)$.

For example, p=13, $a^{25}\equiv a\ (mod\ 26)$ for any integer a.

10). Compute $2222^{5555}+5555^{2222}\ (mod\ 7)$

Solution: $1111\equiv 5\ (mod\ 7)$. $2222^{5555}+5555^{2222}\equiv 3^{5555}+4^{2222}\equiv 3^{5555}+3^{2222}$

$3^6 \equiv 1 \ \Rightarrow 3^{1110} \equiv 1 \ \Rightarrow 3^{2222} \equiv 3^2 \equiv 2, \qquad 3^{5555} \equiv 3^5 \equiv 5 \ (mod\ 7)$

Thus the answer is 0.

11). For any integer a, prove $a^{37} \equiv a \ (mod\ 1729)$.

Solution: $1729 = 7 * 13 * 19$. For each of these 3 prime numbers, by Fermat, we can show $a^{37} \equiv a$ when mod 7, or 13, or 19. (Regardless of a divides the prime or not). Notice 36 is the lcm of 6, 12, and 18.

By Chinese Remainder Theorem, $a^{37} \equiv a \ (mod\ 1729)$.

12). Let p be a prime and p>5, k is a positive integer <p. Prove: the decimal expansion of $\frac{k}{p}$ consists of p-1 repeating decimal digits.

Solution: $10^{p-1} \equiv 1 \ (mod\ p)$. Suppose $10^{p-1} - 1 = mp$, then we have:

$$\frac{k}{p} = \frac{mk}{10^{p-1} - 1}$$

$1 < mk < 10^{p-1} - 1$, this is exactly the form of (p-1) digits looping as a fraction.

13). Let p>5 be a prime, prove $p|111 \ldots 1$ (there are $p-1$ digits)

Solution: $111 \ldots 1 = \frac{1}{9}(10^{p-1} - 1)$, since p is co-prime to 10, thus $p|10^{p-1} - 1$.

14). P is a prime number, show there exist infinitely many integers n such that $p|2^n - n$.

Solution: This is type of "construction" problem, where we need to build such n.

If p is 2, this is true for every even number n. So we focus on odd primes p.

$2^{p-1} \equiv 1\ (mod\ p), \Rightarrow \ 2^{(p-1)^{2k}} \equiv 1$, now notice $(p-1)^{2k} \equiv 1 \ (mod\ p)$.

15). Prove: there are infinitely many prime numbers in form of 4k+1.

Solution: Suppose otherwise, there are only n primes of 4k+1, say they are $p_1, p_2, \ldots, p_n$, now consider $N = 4(p_1 \cdot p_2 \cdot \ldots \cdot p_n)^2 + 1$.

First of all, N co-prime to all the $p_1, p_2, \ldots, p_n$.

And since it is in form of $k^2 + 1$, its prime divisors must be of form 4k+1. And that is a contradiction since all the 4k+1 primes we have listed are not a factor of N.

16). Find the number of positive integers n>1, such that for any integer a, we have $n|a^{25}-a$.

Solution: Suppose S is the set of such integers, and suppose n and m belong to S.

$n|a^{25}-a, m|a^{25}-a \Rightarrow lcm(n,m)|a^{25}-a$. So for any two numbers in S, their lcm is also in S. Thus there must be a maximum element in S, and every other element in S is a divisor of M. We aim to find this maximum element, call it M.

$M|2^{25}-2, M|3^{25}-3$, thus $M|\gcd(2^{25}-2, 3^{25}-3)$.

$2^{25}-2 = 2(2^{12}-1)(2^{12}+1) = 2(2^6-1)(2^6+1)(2^4+1)(2^8-2^4+1)$
$= 2\cdot 7\cdot 9\cdot 5\cdot 13\cdot 17\cdot 241$
$3^{25}-3 = 3(3^{12}-1)(3^{12}+1) = 3(3^6-1)(3^6+1)(3^4+1)(3^8-3^4+1)$
$= 3\cdot(3^2-1)(3^4+3^2+1)(3^2+1)(3^4-3^2+1)\cdot 2\cdot 41\cdot 6481$
$= 3\cdot 8\cdot 7\cdot 13\cdot 2\cdot 5\cdot 73\cdot 2\cdot 41\cdot 6481$
Hence $\gcd(2^{25}-2, 3^{25}-3) = 2\cdot 3\cdot 5\cdot 7\cdot 13$
From Fermat, it is easy to verify $2\cdot 3\cdot 5\cdot 7\cdot 13|a^{25}-a$. Thus $M = 2\cdot 3\cdot 5\cdot 7\cdot 13$. Thus S has 31 elements.

Note: If n has prime divisor p, then $a^{25}\equiv a\ (mod\ p)$, since a is any integer, for any a that is not a multiple of p, we have $a^{24}\equiv 1\ (mod\ p)$. As this is true for any integer a, a good guess would be $p-1|24$, which gives 2, 3, 5, 7, 13.

17). Given odd prime p, for any k=1, 2, 3, ..., p-1, we have:

$$k^{-1}\equiv(-1)^{k-1}\cdot\frac{1}{p}\cdot\binom{p}{k}\qquad (mod\ p)$$

Proof: Multiply k on both sides, and apply $\frac{k}{p}\cdot\binom{p}{k}=\binom{p-1}{k-1}$, we arrived at the following result.

$$\binom{p-1}{k}\equiv(-1)^k\ \ (mod\ p)$$

Note: This provides an alternative way to compute an inverse mod p, via $\binom{p}{k}$ mod p^2.

18). P is an odd prime, a and n>1 are positive integers, with $p^n|a^p-1$, prove $p^{n-1}|a-1$.

Solution: From $p^n|a^p-1$, consider mod p, $a^p\equiv a\equiv 1\ \ (mod\ p)$, thus $p|a-1$.

$a^p-1=(a-1)(a^{p-1}+a^{p-2}+\cdots+a^2+a+1)$, let $A=a^{p-1}+a^{p-2}+\cdots+a^2+a+1$,

$A\equiv 1+1+\cdots+1\equiv 0\ \ (mod\ p)$, we aim to show p^2 does not divide A.

Let $a=kp+1$, with binomial expansion we have:

$A = (kp+1)^{p-1} + (kp+1)^{p-2} + \cdots + (kp+1)^2 + (kp+1) + 1$

$\equiv \binom{p-1}{1} kp + \binom{p-2}{1} kp + \cdots + \binom{2}{1} kp + kp + p \ \ (mod\ p^2)$

$\equiv kp\left[\binom{p-1}{1} + \binom{p-2}{1} + \cdots + \binom{2}{1} + 1\right] + p$

$\equiv kp\dfrac{p(p-1)}{2} + p \equiv p \ \ (mod\ p^2)$

Thus p^2 does not divide A. So $p^{n-1}|a-1$.

19). Lemma. Let p be a prime, then $(a+b)^{p^k} \equiv a^{p^k} + b^{p^k}$ (mod p).

Proof: If k=1, $(a+b)^p = a^p + b^p + \sum \binom{p}{i} a^{p-i}b^i \equiv a^p + b^p$ (mod p).

Now we apply induction, suppose $(a+b)^{p^k} \equiv a^{p^k} + b^{p^k}$, then
$(a+b)^{p^{k+1}} = ((a+b)^p)^{p^k} \equiv (a^p + b^p)^{p^k} \equiv (a^p)^{p^k} + (b^p)^{p^k} \equiv a^{p^{k+1}} + b^{p^{k+1}}$, mod p.

Corollary. Let p be a prime, then $(a+b+c)^{p^k} \equiv a^{p^k} + b^{p^k} + c^{p^k}$ (mod p).

Corollary. Let p be a prime, then $(a_1 + a_2 + \cdots + a_m)^{p^k} \equiv {a_1}^{p^k} + {a_2}^{p^k} + \cdots + {a_m}^{p^k}$ (mod p).

20). For any odd prime p, prove: $1!\,2!\,3!\ldots(p-1)! \equiv (-1)^{\frac{p^2-1}{8}}\left(\dfrac{p-1}{2}\right)! \qquad (\mathrm{mod}\ p)$

Proof: We apply the formula: $k!\,(p-k-1)! + (-1)^k \equiv 0$ (mod p), and make pairs for each k: $1 \le k \le \frac{p-3}{2}$, this gives:

$$\prod_{k=1}^{\frac{p-3}{2}} k! \cdot \prod_{k=1}^{\frac{p-3}{2}} (p-1-k)! \equiv (-1)^{0+1+\cdots+\frac{p-5}{2}} \equiv (-1)^{\frac{p^2-1}{8}-p+2} \equiv -(-1)^{\frac{p^2-1}{8}}$$

Add $\left(\frac{p-1}{2}\right)!\,(p-1)!$, we get $\prod_{k=1}^{p-1} k! \equiv -(-1)^{\frac{p^2-1}{8}}\left(\frac{p-1}{2}\right)!\,(p-1)! \equiv (-1)^{\frac{p^2-1}{8}}\left(\frac{p-1}{2}\right)!$

21). Erdos-Ginzburg-Ziv. Given odd prime p, then for any set of $2p-1$ integers, there exists p elements such that their sum is a multiple of p.

Proof: There are $N = \binom{2p-1}{p}$ such subsets, let their sum be $S_1, S_2, \ldots, S_N$.

If none of them is 0 mod p, then $\sum S_i^{p-1} \equiv 1 * N \equiv \binom{2p-1}{p} \not\equiv 0$ (mod p).

However, if we study the (multi-variate) polynomial

$F(a_1, \dots, a_{2p-1}) = \sum(a_{i_1} + \cdots + a_{i_p})^{p-1}$, we can show each coefficient is 0 mod p.

For a term $a_1^{e_1} a_2^{e_2} \dots a_m^{e_m}$, where $\sum e_i = p-1$, it appears in $\binom{2p-1-m}{p-m}$ sums.

$$For\ all\ m \geq 1, \frac{(p-1)!}{e_1! \cdot e_2! \cdot \dots \cdot e_p!}\binom{2p-1-m}{p-m} \equiv 0 \pmod p$$

Note: The original E.G.Z. theorem is for any n, not just prime p.

22). Carmichael numbers (Pseudo-primes). The converse of Fermat's theorem is not true. Let $n = 561 = 3 \cdot 11 \cdot 17$, we have $n|a^n - a$ for any integer a.

Proof: First, notice $3 - 1|n - 1 = 560$, $11 - 1|n - 1$, and $17 - 1|n - 1$.

For those a that are co-prime to 561, let p be 3 or 10 or 11, then $p|a^{p-1} - 1$ and $a^{p-1} - 1|a^{n-1} - 1$.

If a contains prime divisor p as 3 or 10 or 11, obviously $p|a$ so $p|a^n - a$. We are done.

23). Lemma. Carmichael numbers must be square free. If n satisfies $n|a^n - a$ for any integer a, then n is square free.

Proof: For otherwise, if $k^2|n, k > 1$, let $a = k$, we then have $k^2|k^n - k = k(k^{n-1} - 1)$, the last expression $k(k^{n-1} - 1)$ is obviously not a multiple of k^2.

Theorem. If $n = p_1 \cdot p_1 \cdot \dots \cdot p_r$, where each p are distinct prime numbers, if $p_i - 1|n - 1$ for each p_i, then n is a **Carmichael number**. There are **infinitely many** Carmichael numbers. (561 is the smallest).

Note: Pseudo-primes are very rare, a lot rarer than real primes!

24). Wilson Prime. We know that if p is a prime, then $p|(p-1)! + 1$. If a prime p satisfies $p^2|(p-1)! + 1$, then such prime is called a Wilson Prime. For example 5 and 13 are Wilson primes, 25|4!+1, and 169|12!+1. Remember the following result we proved:

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

Hence Wilson prime satisfies $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p - 1 \pmod{p^2}$.