Recall:

- $x^a - 1 = (x-1)\cdot(x^{a-1} + x^{a-2} + x^{a-3} + \dots + x^1 + 1)$
- $x^{2a+1} + 1 = (x+1)\cdot(x^{2a} - x^{2a-1} + x^{2a-2} - \dots - x^1 + 1)$.

We proved that if 2^m+1 is prime, then $m = 2^n$ for some n.

Suppose 2^m-1 is prime. What can we say about m?

- m must be a prime, otherwise $m = ab$ with $1 < a, b < m$ and $2^m - 1 = (2^b)^a - 1$ is divisible by $2^b - 1$, cannot be prime ($1 < 2^b - 1 < 2^m - 1$)

$F_n = 2^{2^n} + 1$ are called Fermat numbers

$M_p = 2^p - 1$ (p: prime) are called Mersenne numbers.

A proof of infinitude of primes using Fermat numbers:

<u>Lemma:</u> If $a_1, a_2, a_3, \dots$ is a sequence of integers bigger than 1 such that $(a_i, a_j) = 1$ for every $i \neq j$, then there are infinitely many primes dividing the terms of this sequence

Proof: Each term has different prime divisors. Infinitely many terms $\Rightarrow$ Infinitely many prime divisors.

Lemma: $(F_i, F_j) = 1$ for all $i \neq j$.

Proof: Without loss of generality (WLOG) suppose $j > i$ and write $j = i + k$.

$$F_i = 2^{2^i} + 1 \mid 2^{2^{i+1}} - 1 \mid 2^{2^{i+k}} - 1 = F_j - 2$$

$$x = 2^{2^i} \qquad x + 1 \mid x^2 - 1 \mid (x^2)^{2^{k-1}} - 1$$

$\Rightarrow F_i \mid F_j - 2$, i.e. $F_j - 2 = m \cdot F_i$.

$$(F_i, F_j) = (F_i, F_j - m \cdot F_i) = (F_i, 2) = 1.$$

F_i is odd

This proves that n^{th} smallest prime p_n satisfies $p_n \leqslant 2^{2^{n-1}} + 1$. $(p_1 = 2, p_2 = 3, p_3 = 5, \ldots)$.

Modular Arithmetic

Recall that we can partition integers according to their remainders when divided by 4.

$[0]_4 = \{ \ldots, -8, 0, 4, 8, \ldots \}$ $\quad 4k$

$[1]_4 = \{ \ldots, -7, -3, 1, 5, \ldots \}$ $\quad 4k+1$

$[2]_4 = \{ \ldots, -6, -2, 2, 6, \ldots \}$ $\quad 4k+2$

$[3]_4 = \{ \ldots, -5, -1, 3, 7, \ldots \}$ $\quad 4k+3$

- The sum of an element of $[1]_4$ with an element of $[2]_4$ is always in $[3]_4$.
- The product of an element of $[3]_4$ with an element of $[2]_4$ is always in $[2]_4$.

Never depends on the element, the sets determine everything. That means we can do arithmetic with the sets: $[1]_4 + [2]_4 = [3]_4$ or $[2]_4 \cdot [3]_4 = [2]_4$.

There is an easy way to express the rules of summation and multiplication if we also allow using $[-8]_4$, $[12]_4$ etc. for $[0]_4$; $[7]_4$, $[11]_4$ etc for $[3]_4$ ..... (different names for the same set)

Now, $[a]_4 + [b]_4 = [a+b]_4$

$$[a]_4 \cdot [b]_4 = [ab]_4 .$$

Question: When $[a]_4$ and $[b]_4$ are the same set?

Answer: When they have same remainder after division by 4.

$a = 4k + r$ and $b = 4\ell + r \implies a - b = 4(k-\ell)$ is divisible by 4.

Alternative Answer: When $4 \mid a-b$.

When $[a]_4 = [b]_4$ we say a is congruent to b modulo 4 and we write $a \equiv b \pmod 4$.

The general case : mod n $\quad n \in \mathbb{N}$

- Integers are partitioned into n sets (congruence classes)

$\mathbb{Z}_n = \{ [0]_n, [1]_n, [2]_n, \dots, [n-1]_n \}$ and we can do basic arithmetic with the elements of $\mathbb{Z}_n$.

- $[a]_n = [b]_n \iff n \mid a-b$ (same remainder) and we'll say a is congruent to b modulo n and write $a \equiv b \pmod n$ in that case

- $[a]_n + [b]_n = [a+b]_n$; $[a]_n \cdot [b]_n = [ab]_n$.

Are these well-defined operations? We should prove

1. $[a]_n = [c]_n$ and $[b]_n = [d]_n \Rightarrow [a+b]_n = [c+d]_n$

2. $[a]_n = [c]_n$ and $[b]_n = [d]_n \Rightarrow [ab]_n = [cd]_n$.

Proof: $[a]_n = [c]_n \Rightarrow n \mid c-a$

$[b]_n = [d]_n \Rightarrow n \mid d-b$

1. $n \mid c-a$ and $n \mid d-b \Rightarrow n \mid c-a+d-b$
$\Rightarrow n \mid (c+d)-(a+b) \Rightarrow [a+b]_n = [c+d]_n$.

2. $n \mid c-a \Rightarrow c-a = n\cdot k \Rightarrow c = n\cdot k + a$

$n \mid d-b \Rightarrow d-b = n\cdot \ell \Rightarrow d = n\cdot \ell + b$

$cd = (nk+a)\cdot(n\ell+b) = n^2k\ell + nkb + n\ell a + ab$

$\Rightarrow cd - ab = n^2k\ell + nkb + n\ell a = n\cdot(nk\ell + kb + \ell a)$
is divisible by n
$\Rightarrow [cd]_n = [ab]_n$

To summarize some important points.

<u>Theorem:</u> If $a \equiv c \pmod n$ and $b \equiv d \pmod n$, then

- $a+b \equiv c+d \pmod n$
- $ab \equiv cd \pmod n$ $\qquad (k \in \mathbb{N})$
- $a^2 \equiv c^2 \pmod n$, $a^3 \equiv c^3 \pmod n$, ..., $a^k \equiv c^k \pmod n$

Also, we have

- $x \equiv x \pmod n$
- $x \equiv y \pmod n \Rightarrow y \equiv x \pmod n$
- $x \equiv y \pmod n$ and $y \equiv z \pmod n \Rightarrow x \equiv z \pmod n$

Remark: $a \equiv 0 \pmod{n}$ means a is divisible by n.

Why is modular arithmetic a useful tool?

Question: What is the remainder of $113 \cdot 114$ after dividing by 120?

Answer: $113 \equiv -7 \pmod{120}$ and $114 \equiv -6 \pmod{120}$

$\Rightarrow 113 \cdot 114 \equiv (-7) \cdot (-6) \equiv \boxed{42} \pmod{120}$

Question: What is the remainder of 5^{16} after dividing by 17?

Answer: $5^2 \equiv 25 \equiv 8 \pmod{17}$

$5^4 \equiv (5^2)^2 \equiv 8^2 \equiv 64 \equiv -4 \pmod{17}$

$5^8 \equiv (5^4)^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$

$5^{16} \equiv (5^8)^2 \equiv (-1)^2 \equiv \boxed{1} \pmod{17}$

Question: Prove that n^3 is of the form $7k$ or $7k+1$ or $7k+6$.

Solution: $0^3 \equiv 0 \pmod{7}$, $1^3 \equiv 1 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$

$3^3 \equiv 27 \equiv 6 \pmod{7}$, $4^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1 \pmod{7}$

$5^3 \equiv -2^3 \equiv 6 \pmod{7}$, $6^3 \equiv -1^3 \equiv 6 \pmod{7}$

$n^3 \equiv 0^3, 1^3, 2^3, 3^3, 4^3, 5^3$ or $6^3 \pmod 7$ and we are done.

<u>Exercise:</u> $n \in \mathbb{Z}$. Prove that $n \cdot (n+1) \cdot (n+2)$ is divisible by 6.

If $a \equiv b \pmod n$, then

- $3a \equiv 3b \pmod n$
- $2a^2 \equiv 2b^2 \pmod n$
- $a^3 \equiv b^3 \pmod n$

$$\Rightarrow a^3 + 2a^2 + 3a + 5 \equiv b^3 + 2b^2 + 3b + 5 \pmod n$$

More generally,

<u>Theorem:</u> Let $p(x)$ be a polynomial with integer coefficients, then

$a \equiv b \pmod n \implies p(a) \equiv p(b) \pmod n$

(Lemma 3.5 of the textbook)