Chapter- 4

INTRODUCTION TO NUMBER THEORY

PRIME NUMBERS

Prime numbers play a critical role in number theory and in the techniques dis-cussed in this chapter. Table 8.1 shows the primes less than 2000. Note the way the primes are distributed. In particular, note the number of primes in each range of 100 numbers.

Table 8.1 Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t} \qquad \textbf{(8.1)}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer. This is known as the fundamental theorem of arithmetic; a proof can be found in any text on number theory.

$$\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}$$

It is useful for what follows to express this another way. If P is the set of all prime numbers, then any positive integer a can be written uniquely in the following form:

$$a = \prod_{p \in P} p^{a_p} \qquad \text{where each } a_p \geq 0$$

(Product Summation)

The value of any given positive integer can be specified by simply listing all the nonzero exponents in the foregoing formulation.

The integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$.
The integer 18 is represented by $\{a_2 = 1, a_3 = 2\}$.
The integer 91 is represented by $\{a_7 = 1, a_{13} = 1\}$.

It is easy to determine the greatest common divisor[3] of two positive integers if we express each integer as the product of primes.

$$\begin{aligned} 300 &= 2^2 \times 3^1 \times 5^2 \\ 18 &= 2^1 \times 3^2 \\ \gcd(18, 300) &= 2^1 \times 3^1 \times 5^0 = 6 \end{aligned}$$

The following relationship always holds:

If $k = \gcd(a, b)$, then $k_p = \min(a_p, b_p)$ for all p.

FERMAT’S AND EULER’S THEOREMS

Euler’s Totient Function

Before presenting Euler’s theorem, we need to introduce an important quantity in number theory, referred to as **Euler’s totient function**, written $\phi(n)$, and defined as the number of positive integers less than n and relatively prime to n. By convention, $\phi(1) = 1$.

> DETERMINE $\phi(37)$ AND $\phi(35)$.
>
> Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.
>
> To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:
>
> 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18
> 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34
>
> There are 24 numbers on the list, so $\phi(35) = 24$.

Table 8.2 lists the first 30 values of $\phi(n)$. The value $\phi(1)$ is without meaning but is defined to have the value 1.

It should be clear that, for a prime number p,

$$\phi(p) = p - 1$$

Now suppose that we have two prime numbers p and q with $p \neq q$. Then we can show that, for $n = pq$,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$

To see that $\phi(n) = \phi(p) \times \phi(q)$, consider that the set of positive integers less that n is the set $\{1, \ldots, (pq - 1)\}$. The integers in this set that are not relatively prime to n are the set $\{p, 2p, \ldots, (q - 1)p\}$ and the set $\{q, 2q, \ldots, (p - 1)q\}$. Accordingly,

$$\begin{aligned}
\phi(n) &= (pq - 1) - [(q - 1) + (p - 1)] \\
&= pq - (p + q) + 1 \\
&= (p - 1) \times (q - 1) \\
&= \phi(p) \times \phi(q)
\end{aligned}$$

- $\phi(n)$ for $[n \geq 1]$ is defined as the number of +ve integers less than 'n' that are coprime to 'n'.

$$\phi(5) = \{1, 2, 3, 4\} = 4$$

$$\phi(6) = \{1, 5\} = 2$$

- when 'n' is a prime number

$$\phi(n) = n - 1 \quad ; \quad \phi(23) = 22$$

- $\phi(a * b) = \phi(a) * \phi(b)$ [a & b are coprime]

$$\phi(35) = \phi(7 * 5)$$
$$= \phi(7) * \phi(5) \quad [\gcd(7,5) = 1]$$
$$= 6 * 4$$
$$\boxed{= 24}$$

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

For $n = 6$, only the numbers 1 and 5 are **coprime with** 6 so $\varphi(6) = 2$. T
is confirmed by the formula for $n = 6 = 2^1 \times 3^1$, as:

$$\varphi(6) = 6(1 - \frac{1}{2})(1 - \frac{1}{3}) = 2$$

⚠ If n is a prime number, then $\varphi(n) = n - 1$

Table 8.2 Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Euler's Theorem

Euler's theorem states that for every a and n that are relatively prime:

$$a^{\phi(n)} \equiv 1(\text{mod}\, n) \tag{8.4}$$

Proof: Equation (8.4) is true if n is prime, because in that case, $\phi(n) = (n - 1)$ and Fermat's theorem holds. However, it also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as

$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation[6] of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.

2. There are no duplicates in S. Refer to Equation (4.5). If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

which completes the proof. This is the same line of reasoning applied to the proof of Fermat's theorem.

$a = 3; n = 10; \phi(10) = 4 \quad a^{\phi(n)} = 3^4 = 81 = 1 \pmod{10} = 1 \pmod{n}$
$a = 2; n = 11; \phi(11) = 10 \quad a^{\phi(n)} = 2^{10} = 1024 = 1 \pmod{11} = 1 \pmod{n}$

totient f^n.

Note → It is a generalized version of fermat's Theorem.

eg let $x = 11$, $n = 10$ both are coprime

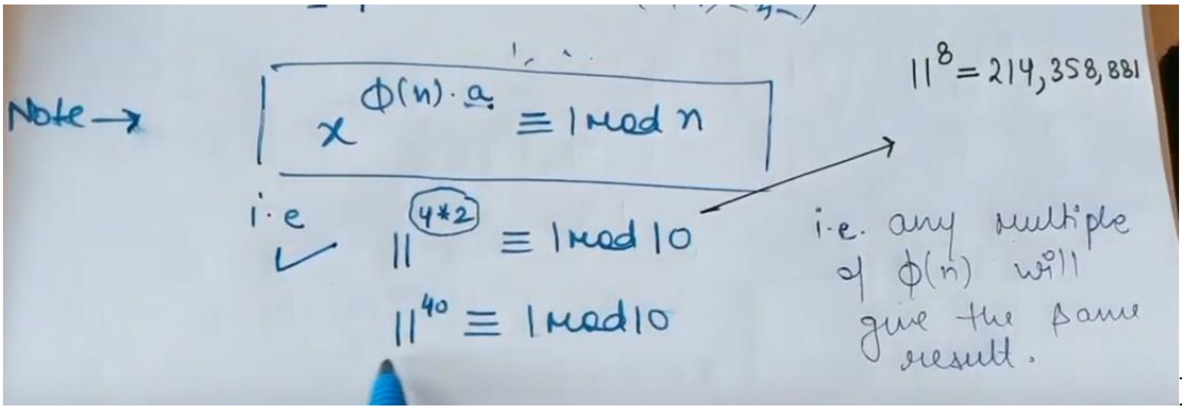
∴ we can represent them as

$11^{\phi(10)} \equiv 1 \bmod 10$

$11^4 \equiv 1 \bmod 10$

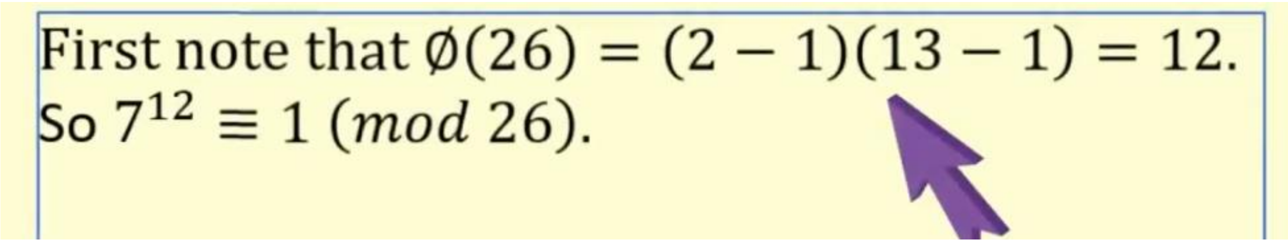
$\boxed{14641 \equiv 1 \bmod 10}$ which is true

$\phi(10) = \phi(2) * \phi(5)$
$= 1 * 4$
$= 4$

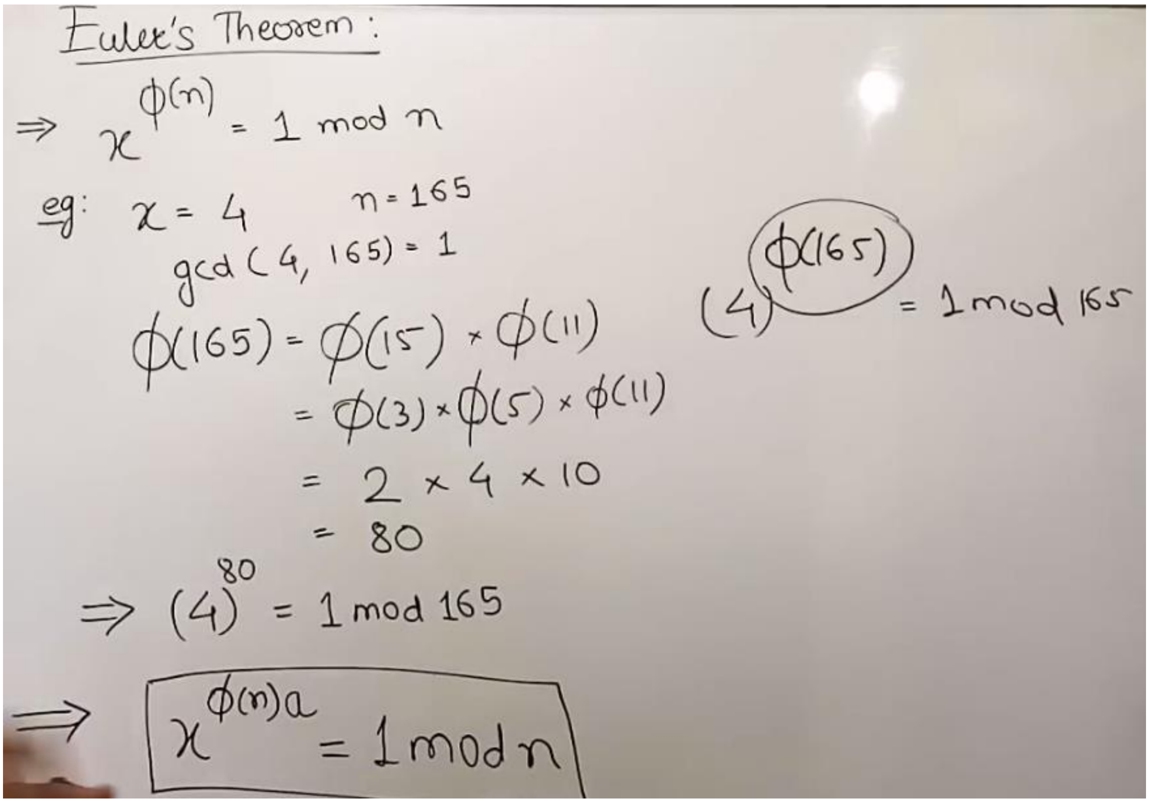


Exercise:

Q. Calculate 7^{133} using Z_{26}



Ans 7 mod 26

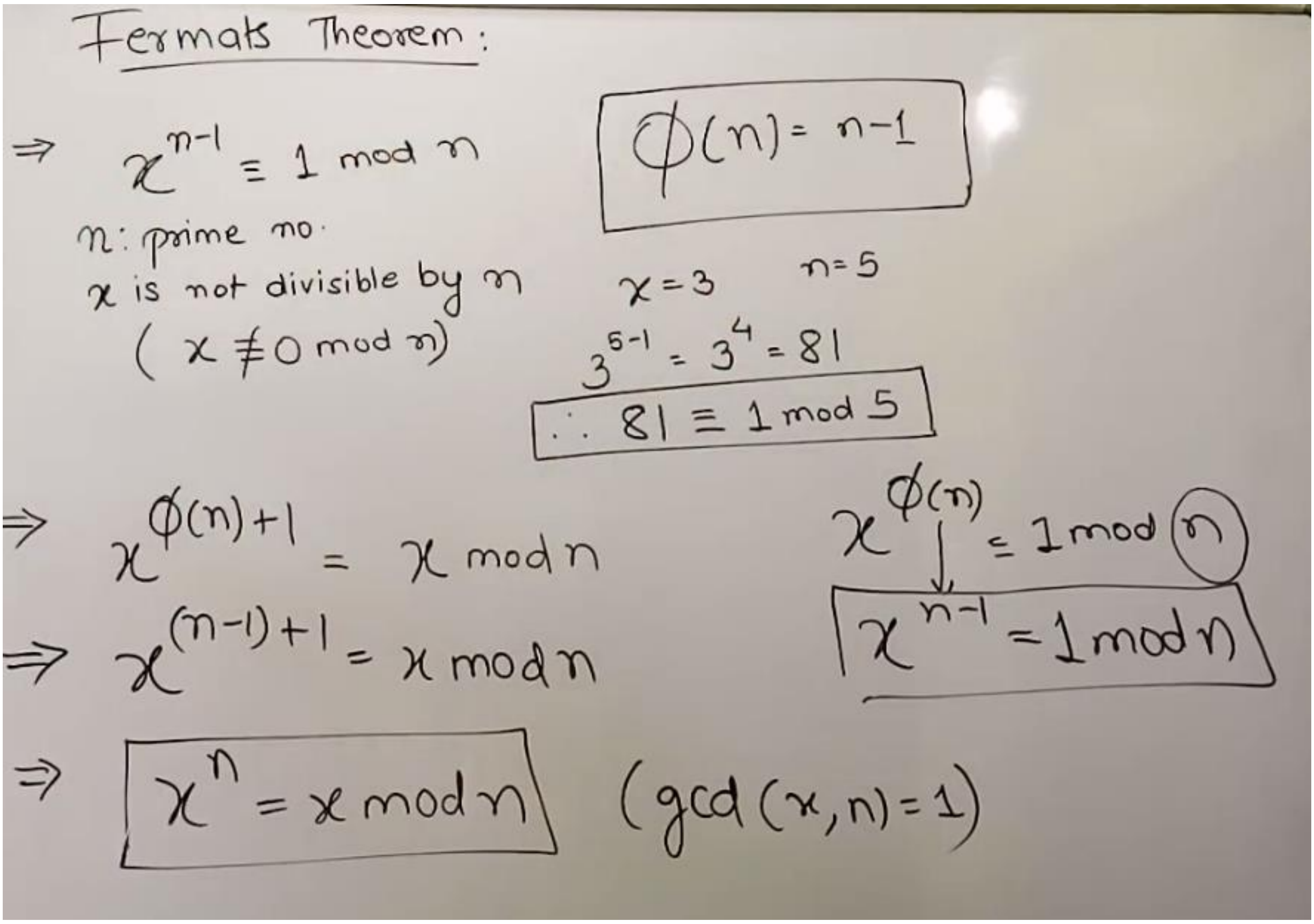


Fermat's Theorem

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p} \qquad \textbf{(8.2)}$$

$a = 7, p = 19$
$7^2 = 49 \equiv 11 \pmod{19}$
$7^4 \equiv 121 \equiv 7 \pmod{19}$
$7^8 \equiv 49 \equiv 11 \pmod{19}$
$7^{16} \equiv 121 \equiv 7 \pmod{19}$
$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$



TESTING FOR PRIMALITY

Miller-Rabin Algorithm[7]

The algorithm due to Miller and Rabin [MILL75, RABI80] is typically used to test a large number for primality. Before explaining the algorithm, we need some background. First, any positive odd integer $n \geq 3$ can be expressed as

$$n - 1 = 2^k q \qquad \text{with } k > 0, q \text{ odd}$$

Miller-Rabin Primality Test

Steps

1) Find $n-1 = 2^k \cdot m$
2) Choose a: $1 < a < n-1$
3) Compute $b_0 = a^m \pmod{n}$, $b_i = b_{i-1}^2$

Example:

Is 53 prime?

1) $n-1 = 2^k \cdot m$ $\quad n = 53$
$53-1 = 2^k \cdot m$ $\quad k, m$ are whole #s

$\frac{52}{2^1} = 26 \;\Big|\; \frac{52}{2^2} = 13 \;\Big|\; \frac{52}{2^3} = \cancel{6.5}$

$52 = 2^2 \cdot 13$ $\qquad k = 2$
$52 = 2^k \cdot m$ $\qquad m = 13$

2) $1 < a < n-1$

$\rightarrow 1 < a < 52$ I pick : $a = 2$

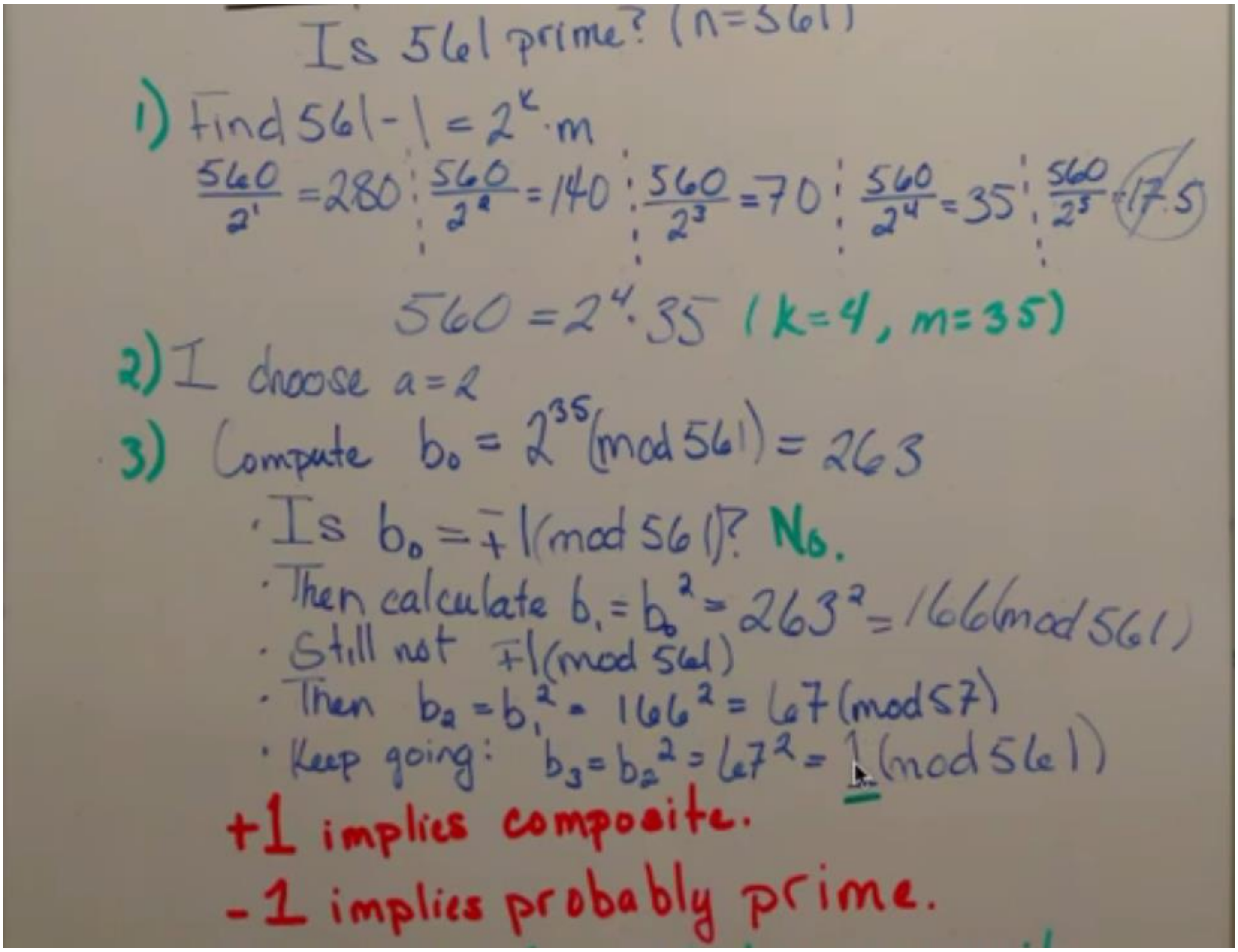
3) $b_0 = a^m \bmod n$

$b_0 = 2^{13} \bmod 53 = 30 \bmod 53$

$b_0 = \begin{cases} +1? \\ -1? \end{cases} \rightarrow$ Prime (probabl

$b_1 = 30^2 \bmod 53 = -1 \bmod 53$

$b_1 = \begin{cases} +1 \rightarrow \text{Composite} \\ -1 \rightarrow \text{Prime} \end{cases}$



THE CHINESE REMAINDER THEOREM

One of the most useful results of number theory is the Chinese remainder theorem (CRT). In essence, the CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.

THEOREM

Chinese Remainder theorem states that there always exists an "x" that satisfies the given congruence.

$$x \equiv rem[0] \pmod{num[0]}$$
$$x \equiv rem[1] \pmod{num[1]}$$

. . . .

and (num[0], num[1] . . . num[n-1]) all must be coprime to ~~each other~~ one another.

one another.

eg.

$$x \equiv 1 \bmod 5$$
$$x \equiv 3 \bmod 7 \rightarrow$$

5 and 7 are coprime

we have to find this $x = 31$

eg

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 4$$
$$x \equiv 1 \bmod 5$$

$gcd(3,4) = gcd(4,5)$
$= gcd(3,5) = 1$
Then only x exists

here $x = 11$

Explain Chienese Remainder Theorem

if
$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

(i) $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1$
ie all coprime

(ii) $x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 + \cdots + M_n X_n a_n) \bmod M$

$$M = m_1 * m_2 * m_3 \cdots m_n$$

$$M = m_1 * m_2 * m_3 \cdots m_n$$

$\boxed{M_i = \frac{M}{m_i}}$ eg $M_1 = \frac{M}{m_1} = \frac{\cancel{m_1} m_2 m_3}{\cancel{m_1}} = m_2 m_3$

$\therefore \boxed{M_1 = m_2 m_3}$

Similarly $\rightarrow M_2 = m_1 m_3 = \frac{M}{m_2} = \frac{m_1 \cancel{m_2} m_3}{\cancel{m_2}} = m_1 m_3$

" $M_3 = m_1 m_2$

To calculate X_i → multiplicative Inverse of M_i

$$M_i X_i \equiv 1 \bmod m_i$$

eg $M_1 X_1 \equiv 1 \bmod m_1$

Theorem

eg $x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 7$ $\longrightarrow$ $x \equiv a_i \bmod (m_i)$
$x \equiv 3 \pmod{11}$

so $a_1 = 1, a_2 = 1, a_3 = 3$
$m_1 = 5, m_2 = 7, m_3 = 11$

Solu $\rightarrow$ Since 5, 7 and 11 all are relatively prime to one another. So, we can find x

i.e $\gcd(5,7) = \gcd(7,11) = \gcd(11,5) = 1$

$$M = m_1 * m_2 * m_3 = 5 * 7 * 11 = 385$$

$$\boxed{M = 385}$$

$$M_1 = \frac{M}{m_1} = m_2 m_3 = 7 * 11 = 77$$

$$M_2 = m_1 m_3 = 5 * 11 = 55$$

$$M_3 = m_1 m_2 = 5 * 7 = 35$$

$M_1 = 77$
$M_2 = 55$
$M_3 = 35$

$= 35$ $M_3 = 35$

Now we will calculate X_i value.

$M_1 X_1 \equiv 1 \pmod{m_1}$ ie $M_1 X_1 \pmod{m_1} = 1$

$77 \cdot X_1 \pmod 5 = 1$

$2 X_1 \pmod 5 = 1$

$$\boxed{\therefore X_1 = 3}$$

Similarly $M_2 X_2 \equiv 1 (\text{mod } m_2)$

$55 X_2 \text{ mod } 7 = 1$

$6 X_2 (\text{mod } 7) = 1$

$\boxed{X_2 = 6}$

$M_3 X_3 \equiv 1 \text{ mod } m_3$

$35 X_3 \equiv 1 \text{ mod } 11$

$2 X_3 \equiv 1 (\text{mod } 11)$

$2 X_3 (\text{mod } 11) = 1$

$\therefore \boxed{X_3 = 6}$

Now, $a_1 = a_2 = 1$ $a_3 = 3$

$m_1 = 5$ $m_2 = 7$ $m_3 = 11$ $M = 385$

$M_1 = 77$ $M_2 = 55$ $M_3 = 35$

$X_1 = 3$ $X_2 = 6$ $X_3 = 6$

$$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \bmod M$$

$$x = (77(3)(1) + 55(6)(1) + 35 \times 6 \times 3) \bmod (385)$$

$$x = (231 + 330 + 630) \bmod 385$$

$$x = 1191 \bmod 385$$

$$\boxed{x = 36}$$

Exercise:

$$x \equiv 1(mod\ 2)$$
$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 5).$$