CHAPTER-9

9.4. If p is a prime number and if a $\not\equiv$ 0 (mod p), then Fermat's Little Theorem tells us that $a^{(p-1)} \equiv 1 \pmod p$.
(a) The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number?
(b) The congruence $129^{64026} \equiv 15179 \pmod{64027}$ is true. Can you conclude that 64027 is a composite number?
(c) The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number?
Answer-

Primality testing

It is extremely difficult to factor large integers (this is the starting point for cryptography). Surprisingly, it is much simpler to tell if a number is a prime or composite (without factoring it). The following is a first hint at how this can be done.

By Fermat's little theorem, if p is a prime, then $a^{p-1} \equiv 1 \pmod p$ for any integer a. On the other hand, this congruence is usually false if p is not a prime.

(a) (1734251 is a composite number)
If 1734251 was a prime, then $7^{1734250} \equiv 1 \pmod{1734251}$.
(a = 7, p = 1734251(although it is not a prime number))
But $1660565 \not\equiv 1 \pmod{1734251}$

(b) (64027 is a composite number☹)
Since a = 129 is not a multiple of 64027, we could use Fermat's Little Theorem if 64027 was a prime.
If 64027 was a prime number, then $129^{64026} \equiv 1 \pmod{64027}$
But **$15179 \not\equiv 1 \pmod{64027}$, therefore 64027 is not a prime number.**

(c) Fermat's little Theorem says, let p is a prime number, and let a be any number with a $\not\equiv 0 \pmod p$. Then

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

But, If it does not give you guarantee that if
$a^{n-1} \equiv 1 \pmod n$ for some $n \in Z$, then n is a prime number.
In this case, n = 52633 is not a prime number. Since n = 7*7519.

CHAPTER-11

Q(6) **For each part, find an x that solves the given simultaneous congruences.**
(a) $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod 9$
(b) $x \equiv 3 \pmod{37}$ and $x \equiv 1 \pmod{87}$
(c) $x \equiv 5 \pmod 7$ and $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$

ANSWER- (a) **The solution to the first congruence consists of all numbers that have the form $x = 7y + 3$ (since $7/(x-3) \Rightarrow x-3 = 7y$ for some y or $x = 7y + 3$)**
We substitute this into the second congruence, simplify, and try to solve.
Thus,

$$7y + 3 \equiv 5 \pmod 9$$
$$7y \equiv 5-3 \pmod 9$$
$$7y \equiv 2 \pmod 9 \qquad ---(1)$$

This is a linear congruence of the form $ax \equiv c \pmod m$. We know how to solve congruence of this sort.
g = gcd(7,9) = 1 and 1 divides c = 2.

The congruence (1) has exactly g = 1 incongruent solution.

Find the solution to the linear equation
$7u + 9v = g = 1$ in integers.
$a = 7, b = 9$
$9 = 1*7 + 2$
$7 = 3*2 + 1$
$2 = 2*1 + 0$

$2 = 9 - 1*7 = b - 1*a = -a + b$
$1 = 7 - 3*2 = a - 3*(-a + b) = 4a - 3b$
$\Rightarrow (u_0 = 4, v_0 = -3)$
$\Rightarrow$ $y_1 = cu_0 / g = 2*4/1 = 8$

1

Solution to the simultaneous congruences is given by $x \equiv 7*y_1 + 3 = 7*8 + 3 = 59 \pmod{9*7=63}$
i.e., $x \equiv 59 (mod\ 63)$ *Ans.*
(How do you know that your answer is correct??)

(b) **The solution to the first congruence consists of all numbers that have the form $x = 37y + 3$ (since $37/(x-3) \Rightarrow x-3 = 37y$ for some y or $x = 37y + 3$)**
We substitute this into the second congruence, simplify, and try to solve.
Thus,

$$37y + 3 \equiv 1 \pmod{87}$$
$$37y \equiv 1-3 \pmod{87}$$
$$37y \equiv -2 \pmod{87}$$

Or $\quad 37y \equiv -2 + 87 \pmod{87}$

Or $\quad 37y \equiv 85 \pmod{87}$ $\quad$ ---(1)

This is a linear congruence of the form $ax \equiv c \pmod m$. We know how to solve congruence of this sort.

g = gcd(37,87) =1 and 1 divides c = 85.

The congruence (1) has exactly g = 1 incongruent solution.

Find the solution to the linear equation
$37u + 87v = g = 1$ in integers.
a = 37, b = 87
87 = 2*37 + 13
37 = 2*13 + 11
13 = 1*11 + 2
11 = 5*2 + 1 = g
2 = 2*1 + 0

13 = 87 – 2*37 = b – 2*a = -2a + b
11 = 37 – 2*13 = a – 2*(-2a + b) = 5a – 2b
2 = 13 – 1*11 = (-2a + b) – 1*(5a – 2b) = -7a +3b
1 = 11 – 5*2 = (5a -2b) – 5*(-7a + 3b) = 40a – 17b
➔ $(u_0 = 40, v_0 = -17)$
⇨ $y_1 = cu_0/g = 85*40/1 = 3400$
or $y \equiv 3400 \pmod{87}$
and $3400 \equiv 7 \pmod{87}$
Therefore, the least residue solution to the linear congruence (1) is given by $y \equiv 7 \pmod{87}$

$x = 37y + 3 = 37*7 + 3 = 262$
Solution to the simultaneous congruences is given by $x \equiv 262 \pmod{37*87=3219}$
i.e., $x \equiv 262 \pmod{3219}$ *Ans.*

(C) **Do yourself.**
(Hint.-)

$x \equiv 5 \pmod 7$
and $x \equiv 2 \pmod{12}$ $\quad$ → **$x \equiv 26 \pmod{7*12=84}$**
and $x \equiv 8 \pmod{13}$ $\quad$ → **$x \equiv 866 \pmod{7*12*13}$**

Q.9 In this exercise you will prove a version of the Chinese Remainder Theorem for three congruences. Let m1, m2, m3 be positive integers such that each pair is relatively prime. That is,

$\gcd(m_1, m_2) = 1$ and $\gcd(m_1, m_3) = 1$ and $\gcd(m_2, m_3) = 1$.
Let a_1, a_2, a_3 be any three integers. Show that there is exactly one integer x in the interval $0 \le x < m_1m_2m_3$ that simultaneously solves the three congruences
$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $x \equiv a_3 \pmod{m_3}$.
Can you figure out how to generalize this problem to deal with lots of
$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ... , $x \equiv a_r \pmod{m_r}$.
In particular, what conditions do the moduli $m_1, m_2, \ldots, m_r$ need to satisfy?

Answer- **Fist find the solution to first two congruences.**
Suppose that $x \equiv b \pmod{m_1m_2}$ is the solution to the first two congruences.
Then find the solution to the simultaneous congruences
$x \equiv b \pmod{m_1m_2}$
and $x \equiv a_3 \pmod{m_3}$.
Suppose the solution is $x \equiv c \pmod{m_1m_2\, m_3}$.
You can easily verify that $x \equiv c \pmod{m_1m_2\, m_3}$ is the unique solution to the simultaneous congruences with $0 \le x < m_1m_2m_3$.

Condition:- $\gcd(m_i, m_j) = 1 \ \forall\, i \neq j$

1- Let $M = m_1m_2m_3 \ldots m_r$ and let $M_i = \dfrac{M}{m_i}$ for $1 \le i \le r$.
Then $M_1 = m_2m_3 \ldots m_r$, $M_2 = m_1m_3 \ldots m_r$, ..., $M_k = m_1m_2\, m_3 \ldots m_{k-1}m_{k+1} \ldots m_r$, ..., $M_r = m_1m_2m_3 \ldots m_{r-1}$
2- Observe that for $1 \le i \le r$, $\gcd(M_i, m_i) = 1$
Hence, for each k, there exists x_k with $1 \le x_k < m_k$ such $M_k x_k \equiv 1 \pmod{m_k}$... (*)
3- Now verify that $x = a_1M_1x_1 + a_2M_2x_2 + \ldots + a_rM_rx_r$ is the required solution.
Notice that $m_i \mid M_j \quad \forall\, i \neq j$
or $\quad mi \mid a_jM_jx_j \quad \forall\, i \neq j$
or $\quad a_jM_jx_j \equiv 0 \pmod{m_i} \quad \forall\, i \neq j$.
Thus $x = a_1M_1x_1 + a_2M_2x_2 + \ldots + a_rM_rx_r \equiv 0 + 0 + \ldots + 1.a_k + 0 + \ldots + 0 \equiv a_k \pmod{m_K}\ \forall\, i \neq j$.
This shows that x is simultaneous solution to the congruences.
Using this you can solve Q.5(c) –
(c) $x \equiv 5 \pmod{7}$ and $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$
$m_1 = 7$, $m_2 = 12$, $m_3 = 13$; $a_1 = 5$, $a_2 = 2$, $a_3 = 8$.
$\gcd(m_1, m_2) = 1$, $\gcd(m_1, m_3) = 1$, $\gcd(m_2, m_3)$.
$M_1 = \frac{m1m2m3}{m1} = 12*13 = 156$, $M_2 = \frac{m1m2m3}{m2} = 7*13 = 91$, $M_3 = \frac{m1m2m3}{m3} = 7*12 = 84$.

Find the solution to
$M_1x \equiv 1 \pmod{m_1}$
$156x \equiv 1 \pmod{7}$

$x_1 = 4$

Find the solution to the linear equation
$156u + 7v = 1$ in integers.
$a = 156$, $b = 7$

$156 = 22*7 + 2$	**$2 = a - 22b$**
$7 = 3*2 + 1$	**$1 = b - 3(a - 22b)$**
	$= -3a + 66b$

$u_0 = -3 \Rightarrow x = 1*(-3)/1 = -3$
$x \equiv -3 \equiv 4 \pmod{7}$, Therefore, $x_1 = 4$.

Find the solution to

$M_2x \equiv 1 \pmod{m_2}$ $\qquad$ $x_2 = 7$

$91x \equiv 1 \pmod{12}$

Find the solution to

$M_3x \equiv 1 (\text{mod } m_3)$ $x_3 = 11$

$84x \equiv 1 \ (\text{mod } 13)$

set $x = a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3$

$= 5*156*4 + 2*91*7 + 8*84*11$

$x \equiv 11786 \ (mod\ m1m2m3)$

or $x \equiv 11786 \ (\text{mod } 1092)$

or $x \equiv 866 (\text{mod } 1092)$ (since $11786 = 10*1092 + 866$)

1. **Start with the list consisting of the single prime {5} and use the ideas in Euclid's proof that there are infinitely many primes to create a list of primes until the numbers get too large for you to easily factor. (You should be able to factor any number less than 1000.)**

([redacted]) Let L_i be the ith list of prime numbers.

$L_1 = \{5\}$

$A = 5+1 = 6 = 2 \times 3$

$q_1 = \min\{2, 3\} = 2$

$L_2 = \{5, 2\}$

$A = 5 \times 2 + 1 = 11 = q_2$

$L_3 = \{5, 2, 11\}$

$A = 5 \times 2 \times 11 + 1 = 111 = 3 \times 37$

$q_3 = \min\{3, 37\}$

$L_4 = \{5, 2, 11, 3\}$

$A = 5 \times 2 \times 11 \times 3 + 1$ Tuesday 2

$= 331 = q_4$

$L_5 = \{5, 2, 11, 3, 331\}$

$A = 5 \times 2 \times 11 \times 3 \times 331 + 1$

$= 109231 \; (> 1000)$

2. (a) **Show that there are infinitely many primes that are congruent to 5 modulo 6. [Hint. Use $A = 6p_1p_2 \cdots p_r + 5$.]**

(b) **Try to use the same idea (with $A = 5p_1\, p_2 \cdots P_r + 4$) to show that there are infinitely many primes congruent to 4 modulo 5. What goes wrong? In particular, what happens if you start with {19} and try to make a longer list?**

(a). Any integer can be congruent to
0, 1, 2, 3, 4, 5 (mod 6).
If an integer is congruent to 0, 2 or 4 (mod 6),
then it is an even number.
Also, an integer congruent to 3 (mod 6)
is divisible by 3.
Thus none of these can represent a prime
greater than 3.
Therefore, if p is a prime number > 3, it
must be either congruent to 1 (mod 6)
or 5 (mod 6).

Suppose that our initial list of primes congruent
to (5 mod 6) is
$$5, p_1, p_2, \ldots, p_r, \quad p_i > 5 \ \forall i = 1, 2, \ldots, r$$

Thursday

Consider the number
$$A = 6p_1p_2 \cdots p_r + 5$$

We know that A can be factored into a
product of primes, say
$$A = q_1q_2 \cdots q_s$$

Claim 1- Among the primes $q_1q_2 \ldots q_s$ at least
one of them must be congruent to
5 (mod 6).
If not, then $q_1q_2 \ldots q_s$ would all be
congruent to 5 (mod 6).

i.e. $A = q_1 q_2 \cdots q_s \equiv 1.1 \ldots 1. \equiv 1 \pmod 6$
which is not possible.

Therefore, one of them, say q, must be congruent to $5 \pmod 6$.

Claim 2. q is different from all p_i's and 5.

Since $p_i \nmid A \;\; \forall\, i = 1, 2, \ldots, r$

and $5 \nmid A$

But $q \mid A$.

Therefore, q is different from 5 and p_i's.

~~Repeat~~ We can include q in our initial list of primes.

Saturday 6

Repeating this process, we can create a list of such primes that is as long as we want.

This shows that there are infinitely many primes that are congruent to $5 \pmod 6$.

(b) $\{p_1, p_2, \ldots, p_r\}$

$A = 5 p_1 p_2 \ldots p_r + 4$

$\{19\}$ and $19 \equiv 4 \pmod 5$

$A = 5 \cdot 19 + 4 = 99 = 3 \times 3 \times 11$

$3 \equiv 3 \pmod 4$ and $11 \equiv 1 \pmod 5$

~~But we donot have any $p_i \equiv 4 \pmod 5$~~ //

CHAPTER- 13

Q(3). The number n! (n factorial) is the product of all numbers from 1 ton. For example, 4! = 1 · 2 · 3 · 4 = 24 and 7! = 1 · 2 · 3 · 4 · 5 · 6 · 7 = 5040. If n > 2, show that all the numbers n! + 2, n! + 3, n! + 4,
are composite numbers.

Q(4). (a) Do you think there are infinitely many primes of the form $N^2 + 2$?
(b) Do you think there are infinitely many primes of the form $N^2 - 2$?
(c) Do you think there are infinitely many primes of the form $N^2 + 3N + 2$?
(d) Do you think there are infinitely many primes of the form $N^2 + 2N + 2$?

Sol^n

$n! = 1 \times 2 \times 3 \times \ldots \times n$

$\therefore \quad n! + 2 = 1 \times 2 \times 3 \times \ldots \times n + 2$

$= 2(1 \times 3 \times 4 \times \ldots \times n + 1)$

$\Rightarrow \quad 2 \mid (n! + 2) \quad \forall \; n \geq 2$

$\therefore$ $n! + 2$ is a composite number.

Similarly, $n! + 3$ is divisible by 3

$n! + 4$ is divisible by 4

$\vdots$

$n! + n$ is divisible by n.

$\therefore$ $n! + 2, n! + 3, \ldots, n! + n$ are composite numbers

8 Monday

Sol^m (a) $N^2 + 2$ (YES)

(b) $N^2 - 2$ (YES)

(c) $N^2 + 3N + 2 = N^2 + 2N + N + 2$

$= N(N+2) + 1(N+2)$

$= (N+2)(N+1)$

$N^2 + 3N + 2$ is divisible by $N+2$ and $N+1$.

(two distinct numbers $\neq 1$ and $N^2 + 3N + 2$)

Therefore, $N^2 + 3N + 2$ can not be a prime number.

(d) $N^2 + 2N + 2$ (YES).

3. The numbers 3^n -1 are never prime (if n $\geq$2), since they are always even. However, it sometimes happens that (3^n -1) /2 is prime. For example, (3^2 -1) /2 = 13 is prime.

(a) Find another prime of the form (3^n -1)/2.

(b) If n is even, show that (3^n - 1)/2 is always divisible by 4, so it can never be prime.

(c) Use a similar argument to show that if n is a multiple of 5 then (3^n - 1)/2 is never a prime.

(d) Do you think that there are infinitely many primes of the form (3n - 1) /2?

(a) Try yourself.

(b). $n = 2k, \quad k \in N$

$$\frac{3^n-1}{2} = \frac{3^{2k}-1}{2}$$

$$= \frac{9^k-1}{2} \qquad -(1)$$

$$(9^k-1) = [(8+1)^k - 1]$$

$$= \left[\left\{\binom{k}{0}8^k + \binom{k}{1}8^{k-1} + \cdots + \binom{k}{k}\right\} - 1\right]$$

$$= \left[\binom{k}{0}8^k + \binom{k}{1}8^{k-1} + \cdots + 1 - 1\right]$$

Friday

$$= \binom{k}{0}8^k + \binom{k}{1}8^{k-1} + \cdots + \binom{k}{k-1}8$$

$$\frac{9^k-1}{2} = \binom{k}{0}4\cdot 8^{k-1} + \binom{k}{1}4\cdot 8^{k-2} + \cdots + \binom{k}{k-1}4$$

$$= 4\left[\binom{k}{0}8^{k-1} + \binom{k}{1}8^{k-2} + \cdots + \binom{k}{k-1}\right]$$

$$\Rightarrow 4 \mid \left(\frac{9^k-1}{2}\right)$$

$$\Rightarrow 4 \mid \frac{3^n-1}{2} \qquad (\text{from } (1))$$

$\Rightarrow \frac{3^n-1}{2}$ can never be a prime number.

(c) $n = 5k \;,\; k \in \mathbb{N}$

$$\frac{3^n - 1}{2} = \left(\frac{3^{5k}-1}{2}\right) = \frac{243^k - 1}{2}$$

$$243^k - 1 = \left[(242+1)^k - 1\right]$$

$$= \left[\left\{\binom{k}{0}(242)^k + \binom{k}{1}(242)^{k-1} + \cdots + \binom{k}{k-1}(242) + \binom{k}{k}\right\} - 1\right]$$

$$= \left[\binom{k}{0}(242)^k + \binom{k}{1}(242)^{k-1} + \cdots + \binom{k}{k-1}242 + 1 - 1\right]$$

Sunday 14

$$= \binom{k}{0}242(242)^{k-1} + \binom{k}{1}(242)(242)^{k-1} + \cdots + \binom{k}{k-1}(242)$$

$$\frac{242^k - 1}{2} = \binom{k}{0}(121)(242)^{k-1} + \binom{k}{1}(121)(242)^{k-2} + \cdots + \binom{k}{k-1}(121)$$

$$= (11)^2\left[\binom{k}{0}(242)^{k-1} + \binom{k}{1}(242)^{k-2} + \cdots + \binom{k}{k-1}\right]$$

$11^2 / \frac{242^k - 1}{2} \Rightarrow \frac{3^{5k}-1}{2}$ or $\frac{3^n - 1}{2}$ can never be a prime number.

5. Prove that a square number can never be a perfect number. [Hint. Compute the value of $\sigma(n^2)$ for the first few values of n. Are the values odd or even?]

Soln

$\sigma(1^2) = \sigma(1) = 1$ (odd)

$\sigma(2^2) = \sigma(4) = 1+2+4 = 7$ (odd)

$\sigma(3^2) = \sigma(9) = \sigma(3.3) = \frac{3^{2+1}-1}{3-1} = 13$ (odd)

$\sigma(4^2) = \sigma(2^4) = \frac{2^{4+1}-1}{2-1} = 31$ (odd).

$\vdots$

Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$\sigma(n^2) = \sigma(p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r})$

$= \sigma(p_1^{2k_1})\, \sigma(p_2^{2k_2}) \cdots \sigma(p_r^{2k_r})$

$(2k_1+1)$ terms

20 Saturday

$= (1+p_1+p_1^2+\cdots+p_1^{2k_1}) \times (1+p_2+\cdots+p_2^{2k_2})$

$\times \cdots \times (1+p_r+\cdots+p_r^{2k_r})$

$=$ (odd number) $\times$ (odd number) $\times \cdots \times$ (odd number)

$=$ odd number

If ~~$\sigma(n^2)$~~ n^2 was perfect number,

$\sigma(n^2) = 2n^2 =$ (even number)

which is not possible.

Therefore, a square number can never be a perfect number.