Tutorial 1.

Q1. Prove that if $gcd(a,b)=1$ and $a|bc$ then $a|c$

$\because$ $gcd(a,b) = 1 \Rightarrow aX + bY = 1$ — (i)

$a|bc \Rightarrow at = bc$ — (ii)

multiplying c on both sides of eq (i) we get

$acX + bcY = c$

using eq (ii) we get

$acX + atY = c$

$a(cX + tY) = c$

$at' = c$

Hence $a|c$

Proved.

Q2. Prove that if a number is relatively prime to two numbers, then it is relatively prime to their product.

let three numbers m, a, b s.t

$gcd(a,m)=1$
$gcd(b,m)=1$ — (i)

need to show $gcd(ab, m) = 1$

$ax + my = 1$
$bx' + my' = 1$ from eq (i)

Now $a \cdot 1 \cdot x + my = 1$

using $1 = bx' + my'$ we get

$= a(bx' + my')x + my = 1$

$= abx'x + may'x + my = 1$

$= abx'x + m(ay'x + y) = 1$

$= ab\hat{X} + m\hat{Y} = 1$

Hence $gcd(ab, m) = 1$ proved.

3. Prove that $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$

Proof: Let $\gcd(m,n) = d$

then $d \mid m$ and $d \mid n$

$dt_1 = m$ and $dt_2 = n$

$\gcd(2^m-1, 2^n-1) = \gcd(2^{dt_1}-1, 2^{dt_2}-1)$

using geometric summation we know

$\frac{2^{dt}-1}{2^d-1} = (1+2^d+\cdots 2^{d(t-1)})$

$\therefore 2^{dt_1}-1 = (2^d-1)(1+2^d+\cdots 2^{d(t_1-1)})$

$2^{dt_2}-1 = (2^d-1)(1+2^d+\cdots 2^{d(t_2-1)})$

$\therefore$ common factor of $2^m-1, 2^{n-1} > 2^d-1$

$\boxed{\gcd \geq 2^d-1}$

$\boxed{p \geq 2^d-1}$ — (i)

Let $\gcd(2^m-1, 2^n-1) = p$

$p \mid 2^m-1 \quad p \mid 2^n-1$

$2^d \equiv 2^{mx+ty} \bmod p$

$\equiv (2^m)^x \bmod p * (2^m)^y \bmod p$

$\equiv 1 \bmod p$

$\therefore 2^d \bmod p \equiv 1$

$\therefore p \mid 2^d-1$

$\therefore \boxed{p \leq 2^d-1}$ — (ii)

From (i) and (ii) we get $p = 2^d-1$

Hence $\gcd(2^m-1, 2^n-1) = 2^d-1 = 2^{\gcd(m,n)}-1$.

Q4. Prove that $\gcd(a^2+m^2, (a-1)^2+m^2) = 1$ if $\gcd(2a-1, 4m^2+1) = 1$

Let $\gcd(a^2+m^2, (a-1)^2+m^2) = t$

using $\gcd(A, B) = \gcd(A, A-B)$

$= \gcd(a^2+m^2, a^2+m^2 - ((a-1)^2+m^2)) = t$

$= \gcd(a^2+m^2, 1-2a) = t$

$= \gcd(a^2+m^2, 2a-1) = t$ using $\gcd(A,-B) = \gcd(A,B)$

Since $2a-1$ is always odd

hence multiplying $2^K(a^2+m^2)$ will have no effect on gcd.

$\therefore \gcd(4(a^2+m^2), 2a-1) = t$

$\gcd(4(a^2+m^2), (2a-1)^2) = t$

$\gcd((2a-1)^2+4(a^2+m^2), (2a-1)) = t$

$\gcd(4a^2+1-4a+4a^2+4m^2, 2a-1) = t$

$\gcd(4a(2a-1)+4m^2+1, 2a-1) = t$

$\gcd(4m^2+1, 2a-1) = t$

Since it is given $\gcd(2a-1, 4m^2+1) = 1$

Hence $\gcd(a^2+m^2, (a-1)^2+m^2) = 1$.

74 mod 149.

5. Prove that for some positive integer n, if 2^n-1 is prime, then n is prime.

Proof:- Let n be a composite number and factor of n be $n = x.y$

$\therefore \; 2^{x \cdot y}-1$

using Geometric Summation we can show that

$$\frac{(2^x)^y-1}{2^x-1} = (1+2^x+2^{2x}+\cdots+2^{(y-1)x})$$

$$\therefore \; 2^{xy}-1 = (2^x-1)\,(1+2^x+2^{2x}+\cdots 2^{(y-1)x})$$

Hence we have shown $2^{xy}-1$ can be broken down into multiplication of two number Hence composite.

So if 2^n-1 is prime implies n is prime.

Q.E.D.

Q6. Prove that for prime p of the form $4K+3$, p divides (a^2+b^2) iff p divides a and p divides b. Also justify that this property not shared by $p=2$ and by primes of the form $4K+1$.

(i) If $p|a$ and $p|b \Rightarrow p|a^2+b^2$

$\Rightarrow pt_1 = a$ and $pt_2 = b$

$$a^2+b^2$$
$$= (pt_1)^2 + (pt_2)^2$$
$$= p^2(t_1^2+t_2^2)$$
$$\therefore p \mid a^2+b^2$$

(ii) $p \mid a^2+b^2 \Rightarrow p|a$ and $p|b$

$$a^2+b^2 \equiv 0 \mod p$$
$$a^2 \equiv -b^2 \mod p$$

Let $p \nmid a$ hence $\gcd(a,p)=1$

$\therefore a^{-1}$ exists

$$a^2(a^{-1})^2 \equiv -b^2(a^{-1})^2 \mod p$$ Let $y = ba^{-1}$

$$-1 \equiv y^2 \mod p$$

By property for the eqn to have soln p have to be of form $4K+1$.

But since p is of form $4K+3$ hence contradiction

$\therefore p|a$ and thus p also divides b.

e.g. for $P=2$, $a=3$, $b=5$

$p \mid (a^2+b^2) \Rightarrow 2 \mid 34$

still $p \nmid 3$ $p \nmid 5$

Q7. Find three consecutive positive integers which are not square free. A number n is said to be square free if it is not divisible by m^2 for any $m > 1$

Let us choose $9 = 3^2$, $16 = 4^2$, $25 = 5^2$

Hence Acc to Ques:- Let n be first number

$$n = 0 \bmod 9$$
$$n+1 = 0 \bmod 16 \equiv n \equiv -1 \bmod 16$$
$$n+2 = 0 \bmod 25 \equiv n \equiv -2 \bmod 25$$

Now using Chinese remainder theorem to solve the eqn we get

$N = 9 * 16 * 25$

$N_1 = 16 * 25$, $a_1 = 0$, $Z_1 = (16 * 25)^{-1} \bmod 9$
$N_2 = 9 * 25$, $a_2 = -1$, $Z_2 = (9 * 25)^{-1} \bmod 16$
$N_3 = 9 * 16$, $a_3 = -2$, Z_3 $(9 * 16)^{-1} \bmod 25$

$$\left(\sum_{i=1}^{3} N_i a_i Z_i \right) \bmod N$$

$= 400 * 0 * 7 + 225 * (-1) * (1) + 144 * (-2) * (4)$

$= -225 - 1152$

$= (-1377) \bmod 3600$

$= 2223$

$\therefore$ $n = 2223$
$n+1 = 2224$
$n+2 = 2225$

verification : $2223 \equiv 0 \bmod 9$
$2224 \equiv 0 \bmod 16$
$2225 \equiv 0 \bmod 25$

8. Find a primitive root of prime 13.

If order of 'a' number 'K' is such that $a^K = 1 \bmod 13$. where K is smallest number and $K = \phi(13)$ then a is primitive root of 13.

$\phi(13) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Let $a = 1$

then $a^1 \bmod 13 \equiv 1 \bmod 13$ Hence not primitive root

$a = 2$.

$2^1 \equiv 2 \bmod 13$

$2^2 \equiv 4 \bmod 13$

$2^3 \equiv 8 \bmod 13$

$2^4 \equiv 3 \bmod 13$

$2^5 \equiv 6 \bmod 13$

$2^6 \equiv 12 \bmod 13$

$2^7 \equiv 11 \bmod 13$

$2^8 \equiv 9 \bmod 13$

$2^9 \equiv 5 \bmod 13$

$2^{10} \equiv 10 \bmod 13$

$2^{11} \equiv 7 \bmod 13$

$2^{12} \equiv 1 \bmod 13$ Hence $a = 2$ is primitive root

Since we have found one primitive root, hence we can find all other primitive root by 2^K where K is coprime to $\phi(13)$

$\therefore$ co-prime of 12 i.e 1, 5, 7, 11

$\therefore$ other primitive roots = $2^5 \bmod 13 = 6$

$2^7 \bmod 13 = 11$

$2^{11} \bmod 13 = 7$

Primitive roots of 13 = $\{2, 6, 11, 7\}$.

9. Find the least non-negative residue of $19! + (13!)^{44} \bmod 23$

We will use Wilson's theorem $(p-1)! = -1 \bmod p$

and fermat's theorem $x^{n-1} \equiv 1 \bmod n$

USING :-
$\phi(n) = 22$
$22! = -1 \bmod 23$
or
$22! = 22 \bmod 23$

$$19! + (13!)^{44} \bmod 23$$

$$= (19! \bmod 23 + (13!)^{44} \bmod 23) \bmod 23$$

$$= (20^{-1} * 21^{-1} * 22^{-1} * (22)! \bmod 23 + ((13!)^{22})^{2} \bmod 23) \bmod 23$$

$$(20^{-1} * 21^{-1} * 22^{-1} * 22 \bmod 23 + 1 \bmod 23) \bmod 23$$

$$= (20^{-1} * 21^{-1} \bmod 23 + 1 \bmod 23) \bmod 23$$

$$= (165 \bmod 23 + 1 \bmod 23) \bmod 23$$

$$= (4 \bmod 23 + 1 \bmod 23) \bmod 23$$

$$= 5 \bmod 23$$

10. Find $\phi(125)$. Let $N = 3^{10!} - 1$. Is N divisible by

$125 = 5^3$

$\phi(5^3) = 5^3 - 5^2 = 125 - 25 = 100$

Divisibility by 125.

if $3^{10!} - 1$ is divisible by 125

then $3^{10!} \bmod 125 \equiv 1 \bmod 125$

using Euler-fermat theorem i.e $x^{\phi(n)} \equiv 1 \bmod n$

$$x^{100} \equiv 1 \bmod 125$$

$$\therefore 3^{10!} \bmod 125 \equiv (3^{100})^{9 \times 8 \times 7 \times 6 \times 4 \times 3 \times 1} \bmod 125 \equiv 1 \bmod 125$$

Hence $3^{10!} - 1$ is divisible by 125.

11. Let g be a primitive root ~~29~~ modulo 29.

(i) How many primitive roots are there modulo 29?

If g is a primitive roots then g^k is also primitive root if K is co-prime to $\phi(n)$.

$\phi(29) = 28$

primitive roots modulo $29 = \phi(28)$

$\phi(28) = 2^2 * 7$

$= (2^2 - 2^1) * 6 = 12.$

(ii) Find a primitive root g modulo 29.

Set $= \{1, 2, 3, 4 \ldots\ldots 28\}$ are all co-prime to 29.

Let $a = 2$

$2^1 \equiv 2 \bmod 29$
$2^2 \equiv 4 \bmod 29$
$2^3 \equiv 8 \bmod 29$
$2^4 \equiv 16 \bmod 29$
$2^5 \equiv 3 \bmod 29$
$2^6 \equiv 6 \bmod 29$
$2^7 \equiv 12 \bmod 29$
$2^8 \equiv 24 \bmod 29$
$2^9 \equiv 19 \bmod 29$
$2^{10} \equiv 9 \bmod 29$
$2^{11} \equiv 18 \bmod 29$
$2^{12} \equiv 7 \bmod 29$
$2^{13} \equiv 14 \bmod 29$
$2^{14} \equiv 28 \bmod 29$
$2^{15} \equiv 27 \bmod 29$
$2^{16} \equiv 25 \bmod 29$
$2^{17} \equiv 21 \bmod 29$
$2^{18} \equiv 13 \bmod 29$
$2^{19} \equiv 26 \bmod 29$
$2^{20} \equiv 23 \bmod 29$
$2^{21} \equiv 17 \bmod 29$
$2^{22} \equiv 5 \bmod 29$
$2^{23} \equiv 10 \bmod 29$
$2^{24} \equiv 20 \bmod 29$
$2^{25} \equiv 11 \bmod 29$
$2^{26} \equiv 22 \bmod 29$
$2^{27} \equiv 15 \bmod 29$
$2^{28} \equiv 1 \bmod 29$

Since order of '2' is $28 = \phi(29)$ Hence '2' is the primitive ~~m~~ root modulo of 29.

(iii) Use primitive root g mod 29 to express all quadratic residue mod 29 as power of g.

we know that '2' is primitive root modulo 29

Hence '2' is the generator.

to get other primitive root we need to find set 'S' where $\forall K \in S$ $\gcd(K, \phi(n)) = 1$

i.e all element in set S are coprime to $\phi(n)$.

$\phi(n) = 28$

$S = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$

$|S| = 12$ $\therefore$ Total 12 primitive root modulo 29 exists

$2^1 \bmod 29 = 2$

$2^3 \bmod 29 = 8$

$2^5 \bmod 29 = 3$

$2^9 \bmod 29 = 19$

$2^{11} \bmod 29 = 18$

$2^{13} \bmod 29 = 14$

$2^{15} \bmod 29 = 27$

$2^{17} \bmod 29 = 21$

$2^{19} \bmod 29 = 26$

$2^{23} \bmod 29 = 10$

$2^{25} \bmod 29 = 11$

$2^{27} \bmod 29 = 15$

Hence 2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15 are all primitive root modulo 29.

(iv) Use the primitive root g mod 29 to express all the quadratic residue modulo 29 as power of g.

Quadratic residue modulo n is
if $x^2 = a \bmod n$ then $a \in Q_n$
Let primitive root g mod 29 = 2
Quadratic residue mod 29 is
$\{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$

$2^{28} \equiv 1 \bmod 29$
$2^{2} \equiv 4 \bmod 29$
$2^{22} \equiv 5 \bmod 29$
$2^{6} \equiv 6 \bmod 29$
$2^{12} \equiv 7 \bmod 29$
$2^{10} \equiv 9 \bmod 29$
$2^{18} \equiv 13 \bmod 29$

$2^{4} \equiv 16 \bmod 29$
$2^{24} \equiv 20 \bmod 29$
$2^{26} \equiv 22 \bmod 29$
$2^{20} \equiv 23 \bmod 29$
$2^{8} \equiv 24 \bmod 29$
$2^{16} \equiv 25 \bmod 29$
$2^{14} \equiv 28 \bmod 29$

If g is primitive root mod p, then $Q_p \equiv g^{2K}$ where $K = 0, 1, \ldots \left(\frac{p-1}{2}\right)$

(v) Find all quadratic residue modulo 29, and all quadratic non ~~set~~ residue modulo 29

For set S $\{1, 2, 3, \ldots\ldots 28\}$ and $x \in S$ and $x^2 \equiv a \bmod 29$ then $a \in Q_{29}$ [Quadratic residue]
else $\in \overline{Q}_{29}$ [Quadratic Non-residue]

Quadratic residue : g^{2n} for $n = 1 \ldots \frac{p-1}{2}$

$Q_n = \{4, 16, 6, 24, 9, 7, 28, 25, 13, 23, 5, 20, 22, 1\}$

Quadratic Non residue :

$\overline{Q}_n = \{2, 8, 3, 12, 19, 18, 14, 27, 21, 26, 17, 10, 11, 15\}$

(vi) Is 5 a quadratic residue modulo 29? If, so is 5 congruent to a fourth power modulo 29?

By Lendgre's symbol $\left(\frac{5}{29}\right)$ we can check whether 5 is quadratic residue or not

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & \text{Quadratic residue} \\ -1 & \text{Quadratic non-residue} \\ 0 & n \text{ devide } a. \end{cases}$$

$$\left(\frac{5}{29}\right) = (5)^{\left(\frac{n-1}{2}\right)} = 5^{14} \bmod 29$$

$$\left(\frac{5}{29}\right) = 1$$

Hence 5 lies in Quadratic residue modulo 29.

To check fourth power modulo 29, we take $a^4 \bmod 29$ $\forall a \in \{1, 2, 3 \ldots 14\}$

So we get $= \{1, 16, 23, 24, 20, 7, 25\}$

Hence 5 is NOT congruent to fourth power modulo 29.

(viii) Use primitive root g mod 29 to calculate all the congruence class that are congruent to fourth powers

(i) class of fourth power modulo 29 are we generate congruence class using generator '2'.

$2^4 \equiv 16 \mod 29$

$2^8 \equiv 24 \mod 29$

$2^{12} \equiv 7 \mod 29$

$2^{16} \equiv 25 \mod 29$

$2^{20} \equiv 23 \mod 29$

$2^{24} \equiv 20 \mod 29$

$2^{28} \equiv 1 \mod 29$

(viii) Show that equation $x^4 - 29y^4 = 5$ has no integral solution.

$x^4 - 29y^4 = 5$

Taking mod 29 on both sides to convert eqn to congruence.

$\therefore (x^4 - 29y^4) \bmod 29 \equiv 5 \bmod 29$

$\Rightarrow (x^4 - 0) \bmod 29 \equiv 5 \bmod 29$

$\Rightarrow x^4 \equiv 5 \bmod 29$

Since we showed 5 is not congruent to fourth power modulo 29. Hence above eqn have no solution.

(vi) / ~~Is 5 a quadratic res~~

12. Simplify $146!$ mod (149) to a number in range $\{0, 1, 2 \cdots 148\}$.

By wilson's theorem we know that if p is prime then

$$(p-1)! \equiv -1 \bmod p$$

$$146! = 148^{-1} * 147^{-1} * (148)!$$

$$\therefore 146! \bmod 149 \equiv 148^{-1} * 147^{-1} * (148)!$$

$$= 148^{-1} * 147^{-1} * (-1) \bmod 149$$

$$= 148^{-1} * 147^{-1} * 148 \bmod 149$$

$$= 147^{-1} \bmod 149$$

$$= 74 \bmod 149.$$