(Section 9.4)

## "Quadratic Congruences with Composite Moduli"

**Theorem (9.11)** If 'p' is an odd prime & $\gcd(a,p)=1$ then congruences $x^2 \equiv a \pmod{p^n}$ ; $n \geq 1$ has a solution if and only if $(a/p)=1$

(proof) If $x^2 \equiv a \pmod{p^n}$ has a solution then $x^2 \equiv a \pmod{p}$ also has a solution (since $n \geq 1$)

Since $\gcd(a,p)=1$

$\Rightarrow \gcd(x,p)=1$

Now, $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$ (by Fermat's theorem)

thus, $a^{(p-1)/2} \equiv 1 \pmod{p}$

$\Rightarrow$ 'a' is a quadratic residue of p (by theorem 9.1)

Hence $(a/p)=1$ (by defⁿ of legendre's symbol)

Conversly, suppose that $(a/p)=1$

Claim: $x^2 \equiv a \pmod{p^n}$ is solvable

we will show by induction

If $n=1$, then it is trivial (i.e If $(a/p)=1$ $\Rightarrow x^2 \equiv a \pmod{p}$ has a solution)

Now, suppose result holds for $n=k \geq 1$

So that $x^2 \equiv a \pmod{p^k}$ admits a solution say $x_0$

then $x_0^2 \equiv a \pmod{p^k}$

$\Rightarrow x_0^2 - a \equiv b p^k$, for some integer b.

$\Rightarrow x_0^2 \equiv a + b p^k$ — (*)

we prove for $n=k+1$

For this, we first solve the linear congruence

$$2x_0 y \equiv -b \pmod{p} \quad -①$$

Since $\gcd(2x_0, p)=1$ & $1 \mid (-b)$

∴ ① has unique solution say $y_0$



Scanned with CamScanner

Now, consider the integer $x_1 = x_0 + y_0 p^k$

$\Rightarrow (x_0 + y_0 p^k)^2 = x_0^2 + 2 x_0 y_0 p^k + y_0^2 p^{2k}$

$= (a + bp^k) + 2 x_0 y_0 p^k + y_0^2 p^{2k}$ (from *)

$= a + (b + 2 x_0 y_0) p^k + y_0^2 p^{2k}$ — ②

Also $p \mid (b + 2 x_0 y_0)$ (by ①)

from ②, we get $p^{k+1} \mid (b + 2 x_0 y_0)$

& $p^{k+1} \mid y_0^2 p^{2k}$

∴ $x_1^2 = (x_0 + y_0 p^k)^2$

$\Rightarrow x_1^2 \equiv a \pmod{p^{k+1}}$ (Using ②)

Thus, the congruence $x^2 \equiv a \pmod{p^n}$ has a solution for $n = k+1$

Hence, by induction, $x^2 \equiv a \pmod{p^n}$ has a solution for all positive integer $n$.

Theorem (9.12) Let 'a' be an odd integer, then

(i) $x^2 \equiv a \pmod 2$ always has a solution

(ii) $x^2 \equiv a \pmod 4$ has a solution if and only if $a \equiv 1 \pmod 4$

(iii) $x^2 \equiv a \pmod{2^n}$, for $n \geq 3$, has a solution if and only if $a \equiv 1 \pmod 8$

Proof (i) Let 'a' be an odd integer

∴ $\gcd(a, 2) = 1$

i.e a is of form $2k+1$

thus, $x^2 \equiv a \pmod 2$ has a solution.



Scanned with CamScanner

(ii) $x^2 \equiv a \pmod 4$

can be solved only when $a$ is of form $4k+1$

∴ there are two solutions modulo 4

namely $x = 1$ & $x = 3$

Consequently, square of any odd integer is congruent to 1 modulo 4.

(iii) Consider $n \geq 3$

Since, the square of any odd integer is congruent to 1 (modulo) 8

∴ $x^2 \equiv a \pmod{2^n}$ is solvable if $a = 8k+1$

Conversely, Now, let $a \equiv 1 \pmod 8$ & proceed by induction on $n$.

When $n = 3$, the congruence $x^2 \equiv a \pmod{2^n}$ is certainly solvable, indeed each of integers $1, 3, 5, 7$ satisfies $x^2 \equiv 1 \pmod 8$

Fix a value of $n \geq 3$ and assume for the induction hypothesis,

i.e congruence $x^2 \equiv a \pmod{2^n}$ admits a solution $x_0$

then $\exists$ an integer 'b' for which $x_0^2 = a + b2^n$ — (1)

Since 'a' is odd, so the integer $x_0$

it is therefore possible to find a unique solution $y_0$ of linear congruence

$$x_0 y \equiv -b \pmod 2$$

Claim: $x^2 \equiv a \pmod{2^{n+1}}$ has a solution say

$$x_1 \equiv x_0 + y_0 2^{n-1}$$

Consider, $(x_0 + y_0 2^{n-1})^2 = x_0^2 + x_0 y_0 2^n + y_0^2 2^{2n-2}$

$= a + b2^n + x_0 y_0 2^n + y_0^2 2^{2n-2}$ (by (1))

$= a + (b + x_0 y_0) 2^n + y_0^2 2^{2n-2}$



Scanned with CamScanner

we get $2 \mid (b + x_0 y_0)$

$\therefore 2^{n+1} \mid (b + x_0 y_0) 2^n$

$\Rightarrow x_1^2 = (x_0 + y_0 2^{n-1})^2 \equiv a \pmod{2^{n+1}}$

Hence, by Induction

$x^2 \equiv a \pmod{2^n}$ for $n \geq 3$ has a solution iff $a \equiv 1 \pmod 8$

Theorem (9.13) Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ be prime factorization of $n > 1$. Let $\gcd(a, n) = 1$ then $x^2 \equiv a \pmod n$ is solvable if and only if

(a) $(a/p_i) = 1$ for $i = 1, 2, \ldots r$

(b) $a \equiv 1 \pmod 4$ if $4 \mid n$ but $8 \nmid n$; $a \equiv 1 \pmod 8$ if $8 \mid n$.

Exercise (9.4)

(Q-1) (a) Show that 7 & 18 are the only congruent solutions of $x^2 \equiv -1 \pmod{25}$

(Solution) By theorem 8.12

$x^k \equiv -1 \pmod{25}$ has a solution

iff $(-1)^{\phi(25)/d} \equiv 1 \pmod{25}$

where $\phi(25) = 20$, $d = \gcd(k, \phi(25))$

Here $k = 2$, $d = \gcd(2, 20) = 2$

$\therefore (-1)^{20/2} = 1 \equiv 1 \pmod{25}$

$\therefore$ it has solution & ~~theorem~~ theorem 8.12 says it has exactly $d = 2$ incongruent solutions

$7 \not\equiv 18 \pmod{25}$ & $7^2 = 49 \equiv -1 \pmod{25}$

& $18^2 = 324 = 24 \equiv -1 \pmod{25}$

First, we solve for $p^{k-1}$ to get $x_0$ & $b$

$\therefore x^2 \equiv -1 \pmod 5$

or $x^2 = 4 \pmod 5$

$x_0 \equiv 2 \pmod 5$, $x_0^2 = 4 = -1 + (1)5$

$\therefore x_0 = 2$, $b = 1$



Scanned with CamScanner

Now, Solve

$2x_0 y \equiv -b \pmod{5}$

or $4y \equiv -1 \pmod{5}$ $(x_0 = 2)$

$\therefore y \equiv +1 \pmod{5}$ $(\gcd(4,5) = 1)$

$\therefore x_1 = x_0 + y_0 p^{k-1}$

$= 2 + 1(5)$

$= 7$ is solution

$x_1 = 7$ is solution to $x^2 \equiv -1 \pmod{5^2}$ & so, $-7$ is also

i.e. $-7 \equiv 18 \pmod{5^2}$

$\therefore x = 7, 18 \pmod{5^2}$

(b) Use part (a) to find solutions of $x^2 \equiv -1 \pmod{5^3}$

(Solution) solve $x^2 \equiv -1 \pmod{5^2}$

(Step 1) from part (a), we get $x_0 = 7$

$\therefore x_0^2 = a + bp^2$

or $7^2 = (-1) + b(5^2)$

$\Rightarrow 49 = (-1) + 2(5^2)$ $(\because b = 2)$

(Step 2) Solve $2x_0 y \equiv -b \pmod{p}$

$\Rightarrow 2(7)y \equiv -b \pmod{p}$

$\Rightarrow 14y \equiv -2 \pmod{5}$

$\Rightarrow -y \equiv -2 \pmod{5}$

$\Rightarrow y \equiv 2 \pmod{5}$

(Step 3) $x_1 = x_0 + y_0 p^2$

$= 7 + 2(5^2) = 57$

$x_1 = 57, -57 \pmod{5^3}$

$= 57, -57 \pmod{5^3}$

$= 57, 68$

By thm 8.12, $d = \gcd(k, \phi(5^3))$

$= \gcd(2, 100)$

$= 2$

So exactly two solutions.



Scanned with CamScanner