Computer Science & Engineering Department
IIT Kharagpur
Computational Number Theory: CS60094
Lecture IV

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1 Basic Properties of Integers III

1.1 Quadratic Residues

Higher order congruence are more difficult to handle. We shall study a congruence of the form $x^2 \equiv a(\bmod\ n)$ for odd integer $n > 1$. Let us consider a general quadratic congruence $ax^2 + bx + c \equiv 0(\bmod\ p)$, where p is an odd[1] prime and $a \in \mathbb{Z}_p^*$. It is clear that the $gcd(4a, p) = 1$. So we write the congruence as

$$\begin{aligned} 4a(ax^2 + bx + c) &\equiv 0(\bmod\ p) \\ \Rightarrow (2ax)^2 + 2 \cdot 2ax \cdot b + b^2 - (b^2 - 4ac) &\equiv 0(\bmod\ p) \\ \Rightarrow (2ax + b)^2 &\equiv (b^2 - 4ac)(\bmod\ p). \end{aligned}$$

If we substitute y for $2ax + b$ and d for $b^2 - 4ac$, we get $y^2 \equiv d(\bmod\ p)$. If $x \equiv x_0(\bmod\ p)$ is a solution of the original congruence, then $y \equiv 2ax_0 + b(\bmod\ p)$ is a solution of the transformed congruence. Again if $y \equiv y_0(\bmod\ p)$ is a solution of the transformed congruence, then $2ax + b \equiv y_0(\bmod\ p)$, i.e. $2ax_0 \equiv y_0 - b(\bmod\ p)$. The solution of this linear congruence, which always exists as $gcd(2a, p) = 1$, gives the solution of the original congruence. In general we are interested about odd positive integer n.
Definition 1: Let n be an odd positive integer. An integer a is called a *quadratic residue modulo n*, if $gcd(a, n) = 1$ ($a \bmod n$ belongs to $\mathbb{Z}_n^*$) and there is an integer b such that $a \equiv b^2(\bmod\ n)$, then $x \equiv b(\bmod\ n)$ is a solution of $x^2 \equiv a(\bmod\ n)$, and b is called *a square root of a modulo n.*

There are a's that are not relatively prime to n, but satisfies the congruence $b^2 \equiv a(\bmod\ n)$. As an example, $6 \equiv 9^2(\bmod\ 15)$. But 6 is not called *quadratic residue modulo 15. Quadratic residue* and *quadratic non-residue* are defined for elements of $\mathbb{Z}_n^*$. Some of these elements are *quadratic residue* and others are *quadratic non-residue.*

Example 1. We take $n = 13$, a prime number.

$$\begin{aligned} 1 &\equiv 1^2 \equiv 12^2(\bmod\ 13), \\ 3 &\equiv 4^2 \equiv 9^2(\bmod\ 13), \\ 4 &\equiv 2^2 \equiv 11^2(\bmod\ 13), \\ 9 &\equiv 3^2 \equiv 10^2(\bmod\ 13), \\ 10 &\equiv 6^2 \equiv 7^2(\bmod\ 13), \\ 12 &\equiv 5^2 \equiv 8^2(\bmod\ 13), \end{aligned}$$

There are two square roots of all the perfect squares modulo 13. There will always be at least two square roots of 1 modulo n. One is 1 and the other is $n - 1$ as $(n - 1)^2 \equiv 1(\bmod\ n)$. This also tells us that there will be at least two square roots of any perfect squares modulo n.
Note that half of the elements of $\mathbb{Z}_{13}^*$ are perfect squares modulo 13. They are the *quadratic residues* and the remaining half are the *quadratic non-residues.* The collection of *quadratic residues* forms a subgroup of $\mathbb{Z}_n^*$.

Example 2. In the second example let us consider a composite number, $n = 15$.

[1]The case of $p = 2$ is simple as $\mathbb{Z}_2 = \{0, 1\}$. The coefficients a, b can be either 0 or 1. So $x^2 + x + 1 \equiv 0(\bmod\ 2)$ cannot have any solution, but $x^2 + x \equiv 0(\bmod\ 2)$ has two solutions.

The elements of $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

$$\begin{aligned} 1 &\equiv 1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 (\text{mod } 15), \\ 4 &\equiv 2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv (\text{mod } 15), \end{aligned}$$

We observe that only prefect squares modulo 15 are 1 and 4. But each has four square-roots modulo 15. 1 and 4 are the two *quadratic residues* modulo 15. The *quadratic non-residues* are 2, 7, 8, 11, 13, 14.

Example 3. In the third example we take $n = 9$, a power of a prime, where $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$.

$$\begin{aligned} 1 &\equiv 1^2 \equiv 8^2 (\text{mod } 9), \\ 4 &\equiv 2^2 \equiv 7^2 (\text{mod } 9), \\ 7 &\equiv 4^2 \equiv 5^2 (\text{mod } 9), \end{aligned}$$

In this case also there are only two square roots of 1 modulo 9. So there are two square roots of all other perfect squares (quadratic residues) modulo 9. Half of the elements are quadratic residues.
Definition 2: Let $n, m \in \mathbb{Z}$ and $n > 0$,

$$(\mathbb{Z}_n^*)^m = \{a^m : a \in \mathbb{Z}_n^*\},$$

the collection of the m^{th} powers of the elements of $\mathbb{Z}_n^*$.
It is not difficult to prove the following facts

1. $(\mathbb{Z}_n^*)^m$ is a subgroup of $\mathbb{Z}_n^*$.

2. Let $a \in \mathbb{Z}_n^*$ and let $l, m \in \mathbb{Z}$ so that l and m are relatively prime. If $a^l \in (\mathbb{Z}_n^*)^m$, then $a \in (\mathbb{Z}_n^*)^m$.

1.1.1 Quadratic Residue Modulo Odd Prime

We prove following interesting results related to any *odd prime p*.
Proposition 1. For any odd prime p, and $q \in \mathbb{Z}_p^*$, $q^2 \equiv 1 (\text{mod } p)$ if and only if $q = 1$ or $q = p - 1 \equiv -1 (\text{mod } p)$.
Proof: If $q = 1$ or $q = p - 1$, then $1^2 \equiv 1 (\text{mod } p)$ and $(p - 1)^2 \equiv p^2 - 2p + 1 \equiv 1 (\text{mod } p)$.
In the other direction, let $q^2 \equiv 1 (\text{mod } p)$, so $p | (q^2 - 1)$. But then p is prime, so $p | q - 1$ or $p | q + 1$. But $q \in \mathbb{Z}_p^*$, we have either $q - 1 = 0$ or $q + 1 = p$. QED.

Proposition 2. If $q \in (\mathbb{Z}_p^*)^2$, where p is an odd prime, then q has exactly two square roots in $\mathbb{Z}_p^*$.
Proof: Let $q \equiv a^2 (\text{mod } p)$ and also $q \equiv b^2 (\text{mod } p)$. So we have $a^2 \equiv b^2 (\text{mod } p)$. We multiply both sides by $(b^{-1})^2$ (mod$p$) and get $(ab^{-1})^2 \equiv 1 (\text{mod } p)$. By the previous proposition we have $ab^{-1} \equiv 1 (\text{mod } p)$ or $ab^{-1} \equiv p - 1 (\text{mod } p)$. So $a \equiv b (\text{mod } p)$ $a \equiv -b (\text{mod } p)$. So in $\mathbb{Z}_p^*$, $a = \pm b$ i.e. there are exactly two square roots. QED.

Proposition 3. For any odd prime p, the size of $(\mathbb{Z}_p^*)^2$ is $\frac{p-1}{2}$.
Proof: We define the map, $sq : \mathbb{Z}_p^* \to (\mathbb{Z}_p^*)^2, a \mapsto a^2$. Every image has two distinct preimages, so $2|(\mathbb{Z}_p^*)^2| = |\mathbb{Z}_p^*| = p - 1$. QED.

Example 4. Let $p = 11$, $(\mathbb{Z}_{11}^*)^2 = \{1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 5, 5^2 = 3\}$, and $\mathbb{Z}_{11}^* = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$.
If p is an odd prime, half of the elements of $\mathbb{Z}_p^*$ are quadratic residue and other half are quadratic non-residue.
Theorem 4. (*Euler's Criterion*) Let p be an odd prime and $a \in \mathbb{Z}_p^*$.

1. $a^{(p-1)/2} \equiv \pm 1 (\text{mod } p)$,

2. If $a \in (\mathbb{Z}_p^*)^2$ then $a^{(p-1)/2} \equiv 1 (\text{mod } p)$,

3. If $a \notin (\mathbb{Z}_p^*)^2$ then $a^{(p-1)/2} \equiv -1 (\text{mod } p)$,

Proof:

1. Let $b \equiv a^{(p-1)/2} (\text{mod } p)$, so $b^2 \equiv a^{p-1} \equiv 1 (\text{mod } p)$, by Euler's theorem. But we know that if $b^2 \equiv 1 (\text{mod } p)$, then $b \equiv 1, p-1 (\text{mod } p)$.

2. $a \equiv b^2 (\text{mod } p)$. So $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 (\text{mod } p)$.

3. $a \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$.
   We claim that for each $b \in \mathbb{Z}_p^*$ there is a $c \in \mathbb{Z}_p^*$ so that $bc \equiv a (\text{mod } p)$ and $b \neq c$.
   If $b = c$, then $a \equiv b^2 (\text{mod } p)$ and $a \in (\mathbb{Z}_p^*)^2$. Our $c = b^{-1}a$ and it is unique.
   So we have the product of all elements of $\mathbb{Z}_p^*$,

$$\prod_{b,c \in \mathbb{Z}_p^*} (b \times_p c) = a^{(p-1)/2}.$$

   We also claim that for each $b \in \mathbb{Z}_p^*$ there is a $c \in \mathbb{Z}_p^*$ so that $bc \equiv 1 (\text{ mod } p)$. We know that there are only two elements in $\mathbb{Z}_p^*$ whose square is 1. They are 1 and $p-1$. Any other b, c whose product is 1 are distinct.
   So we have another product of all elements of $\mathbb{Z}_p^*$,

$$\left(\prod_{a \in \mathbb{Z}_p^*} a \right) = \left(1 \times_p (-1) \times \prod_{b \times_p c = 1, b \neq c} b \times_p c \right) = -1.$$

   Hence the result.

QED.

Example 5. We consider $p = 13$ and $5 \in \mathbb{Z}_{13}^* \setminus (\mathbb{Z}_{13}^*)^2$.

$$5 = 1 \times_{13} 5 = 2 \times_{13} 9 = 3 \times_{13} 6 = 4 \times_{13} 11 = 7 \times_{13} 10 = 8 \times_{13} 12.$$

Also

$$1 = 2 \times_{13} 7 = 3 \times_{13} 9 = 4 \times_{13} 10 = 5 \times_{13} 8 = 6 \times_{13} 11.$$

So we have $5^{\frac{13-1}{2}} \equiv 1 \times_{13} \times_{13} (-1) \times_{13} 1^{\frac{13-3}{2}} \equiv -1 (\text{mod } 13)$.

The conclusion of the Euler's criterion is

$$a \in (\mathbb{Z}_p^*)^2 \text{ if and only if } a^{(p-1)/2} \equiv 1.$$

We have a byproduct of our earlier proof.

Theorem 5. (*Wilson's Theorem*) If p is a prime, then $(p-1)! \equiv -1 (\text{mod } p)$.
Proof: We have already proved that for an odd prime $\prod_{a \in \mathbb{Z}_p^*} a = -1$. This is also true for 2 where 1 is same as -1 mod 2. QED.

Proposition 6. (*Converse of Wilson's Theorem*) If n is a positive integer greater than 1 and $(n-1)! \equiv -1 (\text{mod } n)$, then n is prime.
Proof: If n is not a prime, then $n = ab$, where $1 < a, b < n$. From the given condition we see that $n | [(n-1)! + 1]$. So $a | [(n-1)! + 1]$. But then $a | (n-1)!$ implies that $a | 1$ - a contradiction. QED.

Proposition 7. Let p be an odd prime and $a, b \in \mathbb{Z}_p^*$. If none of a, b are in $(\mathbb{Z}_p^*)^2$, then $ab \in (\mathbb{Z}_p^*)^2$.
Proof: We have

$$(a \times_p b)^{(p-1)/2} \equiv a^{(p-1)/2} \times_p b^{(p-1)/2} \equiv -1 \times_p -1 \equiv 1 (\text{mod } p).$$

So by the Euler's criterion $ab \in (\mathbb{Z}_p^*)^2$. QED.

1.1.2 Quadratic Residue Modulo Power of Odd Prime

Let p be an odd prime and $k > 0$ be an integer. We are interested about the solution of $x^2 \equiv a(\text{mod } p^k)$ in $\mathbb{Z}_{p^k}^*$. We have already seen characterisation in case of $k = 1$. There are similar theorems for $k > 1$.

Proposition 8. Let p be any odd prime and let k be any positive integer. For all $q \in \mathbb{Z}_{p^k}^*$, $q^2 \equiv 1(\text{mod } p^k)$ if and only if $q = 1$ or $q = p^k - 1 \equiv -1(\text{mod } p^k)$.

Proof: If $q = 1$ or $q = p^k - 1$, then $1^2 \equiv 1(\text{mod } p^k)$ and $(p^k - 1)^2 \equiv p^{2k} - 2p^k + 1 \equiv 1(\text{mod } p^k)$.

In the other direction, let $q^2 \equiv 1(\bmod\ p^k)$, so $p^k|(q^2-1)$, implies $p|(q-1)(q+1)$. p is prime, so $p|q-1$ or $p|q+1$. But p cannot divide both $q-1$ as well as $q+1$; otherwise p divides $(q+1)-(q-1) = 2$. But that is impossible as p is an odd prime. So p^k divides either $q-1$ or $q+1$. But then $q \in \mathbb{Z}_{p^k}^*$. So if $p^k|(q-1)$, then $q - 1 = 0$, and if $p^k|(q+1)$, then $q + 1 = p^k$ i.e. $q = p^k - 1$. QED.

Following sequence of propositions are similar to the case of $k = 1$. We leave them as exercise.

Proposition 9. For any odd prime p and positive integer k, if $q \in (\mathbb{Z}_{p^k}^*)^2$, then q has exactly two square roots in $\mathbb{Z}_{p^k}^*$.

Proposition 10. For any odd prime p and a positive integer k, the size of $(\mathbb{Z}_{p^k}^*)^2$ is $\frac{\phi(p^k)}{2}$.

Proposition 11. (Generalisation of Euler's Theorem)
Let p be an odd prime, k be a positive integer and $a \in \mathbb{Z}_{p^k}^*$.

1. $a^{\phi(p^k)/2} \equiv \pm 1(\text{mod } p^k)$,
2. If $a \in (\mathbb{Z}_{p^k}^*)^2$ then $a^{\phi(p^k)/2} \equiv 1(\text{mod } p^k)$,
3. If $a \notin (\mathbb{Z}_{p^k}^*)^2$ then $a^{\phi(p^k)/2} \equiv -1(\text{mod } p^k)$,

Proposition 12. (Generalisation of Wilson's Theorem)
If p is an odd prime and k is a positive integer, then $\prod_{a \in \mathbb{Z}_{p^k}^*} a \equiv -1(\bmod\ p^k)$.

Proposition 13. Let p be an odd prime and k be a positive integer and $a, b \in \mathbb{Z}_{p^k}^* \setminus (\mathbb{Z}_{p^k}^*)^2$, then $ab \in (\mathbb{Z}_{p^k}^*)^2$.

Finally we have the following interesting proposition.

Proposition 14. If p is an odd prime, k is a positive integer and $a \in \mathbb{Z}_{p^k}^*$, then a is a *quadratic residue modulo* p if and only if it is a *quadratic residue modulo* p^k.

Proof: Let a be a quadratic residue modulo p^k i.e. $gcd(a, p^k) = 1$ and there is an integer b so that $a \equiv b^2(\bmod\ p^k)$. So we have $gcd(a, p) = 1$ and $a \equiv b^2(\bmod\ p)$. So a is quadratic residue (perfect square) modulo p.

Let a is not a quadratic residue modulo p^k. If $p|a$, then a is not a quadratic residue modulo p. So we assume that $p \not| a$. Using the generalised Euler's criterion we have $a^{\phi(p^k)/2} \equiv -1(\text{mod } p^k)$. This implies that $a^{\phi(p^k)/2} \equiv -1(\text{mod } p)$. We use the Fermat's little theorem

$$a \equiv a^p \equiv (a^p)^p \equiv \cdots \equiv a^{p^{k-1}}(\text{mod } p).$$

By substituting we get,

$$-1 \equiv a^{\phi(p^k)/2} \equiv a^{p^{k-1}(p-1)/2} \equiv (a^{p^{k-1}})^{(p-1)/2} \equiv a^{(p-1)/2}(\text{mod } p).$$

So a is a quadratic non-residue modulo p. QED.

1.1.3 Quadratic Residue Modulo n

Now we consider the general case of odd n, a product of odd primes.

Proposition 15. Let n be an odd integer greater than 1. The prime decomposition of $n = p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}$. If $a \in \mathbb{Z}_n^*$ is a perfect square, then a has 2^k square-roots.

Example 6. Let us look at *Example (1.1)* where $n = 15 = 3^1 \times 5^1$. The Chinese Remainder Map is $f : \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$ is $n \mapsto (n \bmod 3, n \bmod 5)$. We know that

there are two perfect squares in $\mathbb{Z}_{15}$ and they are 1 and 4. We have $f(1) = (1, 1)$ and $f(4) = (1, 4)$. There are two square roots of 1 modulo 3, and they are 1 and 2. Similarly there are two square roots of 1 modulo 5, they are 1 and 4. And two square roots of 4 modulo 5, they are 2 and 3.
So $f(1) = (1, 1) = (1^2 \bmod 3, 1^2 \bmod 5) = (1^2 \bmod 3\ , 4^2 \bmod 5) = (2^2 \bmod 3\ , 1^2 \bmod 5) = (2^2 \bmod 3\ , 4^2 \bmod 5)$. If $b^2 \equiv 1 (\bmod\ 15)$, then $f(b^2) = (b^2 \bmod 3, b^2 \bmod 5) = ((b \bmod 3)^2 \bmod 3, (b \bmod 5)^2 \bmod 5)$. As $f(b) = (b \bmod 3, b \bmod 5)$, the values of b are $f^{-1}(1, 1) = 1$, $f^{-1}(1, 4) = 4$, $f^{-1}(2, 1) = 11$ and $f^{-1}(2, 4) = 14$. So the square roots of 1 modulo 15 are $1, 4, 11, 14$.
Proof: We consider the Chinese Remainder Map,

$$f : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

We know that the restriction of f to $\mathbb{Z}_n^*$ is also a *bijection*.

$$f : \mathbb{Z}_n^* \to \mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}.$$

Let $a \in (\mathbb{Z}_n^*)^2$, a perfect square modulo n i.e. $a \equiv b^2 (\bmod\ n)$, for some $b \in \mathbb{Z}_n^*$. We have $f(a) = (a \bmod p_1^{e_1}, \cdots, a \bmod p_k^{e_k}) = (a_1, \cdots a_k) \in \mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}$. Let $f(b) = (b \bmod p_1^{e_1}, \cdots, b \bmod p_k^{e_k}) = (b_1, \cdots, b_k) \in \mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}$.

Note that in a Chinese remainder map, $f : \mathbb{Z}_N \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $\{n_i\}_{i=1}^k$ are pairwise relatively prime, and $N = \prod_{i=1}^k n_i$, $f(xy) = ((xy) \bmod n_1, \cdots, (xy) \bmod n_k) = ((x \bmod n_1)(y \bmod n_1) \bmod n_1, \cdots, (x \bmod n_k)(y \bmod n_k) \bmod n_k) = (x_1 y_1, \cdots, x_k y_k)$.
So we have

$$(a_1, \cdots a_k) = f(a) = f(b^2) = (b_1^2, \cdots, b_k^2).$$

So we have perfect squares $a_i \equiv b_i^2 (\bmod\ p_i^{e_i})$, for all $i = 1, \cdots, k$.

On the other hand, if we have perfect square, $a_i \equiv b_i^2 (\bmod\ p_i^{e_i})$, for all $i = 1, \cdots, k$, then let us call $f^{-1}(b_1, \cdots, b_k) = b \in \mathbb{Z}_n^*$ (the restriction of f is also a bijection). So we have

$$f(b^2) = (b^2 \bmod p_1^{e_1}, \cdots, b^2 \bmod p_k^{e_k}) = (b_1^2, \cdots, b_k^2) = (a_1, \cdots, a_k) = f(a).$$

As f is a bijection, $a \equiv b^2 (\bmod\ n)$ i.e. a is a perfect square in $\mathbb{Z}_n^*$. This shows that

$$a \in (\mathbb{Z}_n^*)^2 \text{ if and only if } a_i \in (\mathbb{Z}^*_{p_1^{e_i}})^2, \text{ for } i = 1, \cdots, k.$$

Each perfect square in $\mathbb{Z}^*_{p_1^{e_i}}$ has two square roots, so a has 2^k square roots.
This gives us the size of $(\mathbb{Z}_n^*)^2$.

$$|(\mathbb{Z}_n^*)^2| = \prod_{i=1}^k |(\mathbb{Z}^*_{p_1^{e_i}})^2| = \prod_{i=1}^k \phi(p_1^{e_i})/2 = \phi(n)/2^k.$$

We formally conclude that any element $a \equiv b^2 \in (\mathbb{Z}_n^*)^2$ has 2^k square roots.
Let $a \equiv b^2 (\bmod\ n)$ and $a \equiv c^2 (\bmod\ n)$. So we have $b^2 \equiv c^2 (\bmod\ n)$. This amounts to saying that $b_i^2 \equiv c_i^2 (\bmod\ n_i)$, for $i = 1, \cdots, k$. So each $b_i \equiv \pm c_i (\bmod\ n_i)$ and there are altogether 2^k possibilities. QED.

1.1.4 Testing of Quadratic Residuosity

We wish to test whether an integer a is *quadratic residue* modulo n. If $gcd(a, n) \neq 1$, then a by definition is not a *quadratic residue* modulo n. So we assume that a and n are relatively prime. We consider the following three cases:

1. *n is an odd prime:* We compute the value of $a^{\frac{p-1}{2}} \bmod n$. This can be done using repeated squaring algorithm given below

   It computes $a^e \bmod n$ where $a \in \mathbb{Z}_n$ and e is a positive integer. Let the binary representation of $e = (e_{k-1} e_{k-2} \cdots e_1 e_0)$.

```
modExpN(a, e, n)
    exp ← 1
    s ← a mod n
    while e ≥ 1
        if (e mod 2) = 1 then exp ← (exp × s) mod n
        s ← s^2 mod n
        e ← e ÷ 2
    return exp
```

$k = \lceil \log_2 e \rceil$, so the loop is executed k times with k *squaring* and $\leq k$ multiplications over $\mathbb{Z}_n$. So the running time is $O(\log e (\log n)^2)$. If $1 < e < n$, then it is $O(\log n)^3)$.
We shall see afterward that there is better method for testing *quadratic residuosity* for an odd prime.

2. $n = p^k$ *where p is an odd prime:* We have already proved that a is a *quadratic residue* modulo p^k if and only if a is a *quadratic residue* modulo p. So this can also be done efficiently.

3. *n is an odd integer:* If the prime factorisation of n is known, then we can use the previous method to determine whether a is a *quadratic residue* modulo p for every prime factor of n. Then using this fact we can conclude about the *quadratic residuocity* of a modulo n (*Chinese remainder theorem*). But if the factorisation is not given, there is no efficient algorithm known to test *quadratic residuocity*. Factorisation is believed to be a hard problem.
We shall see that the computation of *Jacobi symbol*, for which efficient algorithm is known, gives partial answer.

If it is known that a is a *quadratic residue* modulo p, an odd prime, it is necessary to find one b such that $b^2 \equiv a(\bmod\ p)$. We shall address this problem afterward.

1.1.5 Square Roots of $p - 1$

Following theorem characterises the odd primes p such that $p - 1$ or -1 is a *quadratic residue* modulo p. This has some interesting applications.
Proposition 16. Let p be an odd prime. $p - 1 \in (\mathbb{Z}_p^*)^2$ if and only if $p \equiv 1(\bmod 4)$ i.e. $p = 4k + 1$.
Proof: By the Euler's criterion, $p - 1$ is a quadratic residue modulo p if and only if $(p-1)^{(p-1)/2} \equiv 1(\bmod\ p)$. If p is of the form $4k+1$, then $(p-1)/2 = 2k$, an even number. So

$$(p - 1)^{2k} \equiv (-1)^{2k} \equiv 1(\bmod p).$$

If $p \equiv 3(\bmod p)$, then $p = 4k + 3$ and $(p - 1)/2 = 2k + 1$, an odd number. So,

$$(p - 1)^{2k+1} \equiv (-1)^{2k+1} \equiv -1(\bmod p).$$

QED.

Proposition 17. There are infinitely many primes $p \equiv 1(\bmod 4)$.
Proof: Let there be finite number of such primes, $p_1, \cdots, p_k$, and let $n = 4m^2 + 1$, where $m = p_1 \cdots p_k$. Let p be a prime factor of n. Clearly p is not equal to any one of $p_1, \cdots, p_k$. We have $(2m)^2 \equiv -1(\bmod p)$. So -1 is a quadratic residue of p and by our previous theorem, $p \equiv 1(\bmod 4)$. This contradicts our assumption. QED.

Proposition 18. (*Thue's Lemma*) Let p be a prime and a is an integer such that $p \not| a$. There exists two integers x and y, such that (i) $0 < |x|, |y| < \sqrt{p}$, and (ii) $ax \equiv y(\bmod p)$.

Example 7. Let $n = 13$ and $a = 7$. We have $7x = y(\bmod 13)$. $(2, 1)$ is a solution of the congruence satisfying $0 < 1, 2 < \sqrt{13}$.

Proof: Let
$$A = \{au - v : u, v \in \mathbb{Z} \land 0 \leq u, v \leq \lfloor\sqrt{p}\rfloor\}.$$
Clearly there are $\lfloor\sqrt{p}\rfloor + 1$ integers in the interval. So, the number of ordered pairs (u, v) corresponding to the elements of A is greater than p. By the *pigeon-hole principle* there are two distinct ordered pairs (u_1, v_1) and (u_2, v_2) such that $au_1 - v_1 \equiv au_2 - v_2 (\text{mod } p)$. So we have $a(u_1 - u_2) \equiv (v_1 - v_2)(\text{mod } p)$. This gives a solution of $ax \equiv y(\text{mod } p)$, where $x = u_1 - u_2$ and $y = v_1 - v_2$.
Both $|x|, |y| < \sqrt{p}$ (as a prime cannot be a perfect square). If one of x or y is 0, the congruence $ax \equiv y(\text{ mod } p)$ implies that the other one will also be 0. But both $x = u_1 - u_2$ and $y = v_1 - v_2$ cannot be 0 as the ordered pairs are distinct. So both x and y are non-zero. QED.

Theorem 19. (*Fermat*)
An odd prime p is expressible as sum of two squares if and only if $p \equiv 1(\text{mod } 4)$.
Proof: If $p = a^2 + b^2$, then one of a or b is odd and the other one is even. We assume that $a = 2c$ and $b = 2d + 1$. So $a^2 \equiv 0(\text{mod } 4)$ and $b^2 \equiv 1(\text{mod } 4)$, implies that $p = a^2 + b^2 \equiv 1(\text{mod } 4)$.

If $p \equiv 1(\text{mod } 4)$, -1 is a quadratic residue modulo p. So we have an integer a so that $a^2 \equiv -1(\text{mod } p)$, where $gcd(p, a) = 1$.
At this point we invoke the Thue's lemma. There is a solution (X_0, Y_0) of $ax \equiv y(\text{mod } p)$ such that $0 < |X_0|, |Y_0| < \sqrt{p}$. So we have

$$\begin{aligned}
aX_0 &\equiv Y_0(\text{mod } p), \\
(aX_0)^2 &\equiv Y_0^2(\text{mod } p), \\
a^2X_0^2 &\equiv Y_0^2(\text{mod } p), \\
-X_0^2 &\equiv Y_0^2(\text{mod } p),\ a^2 \equiv -1(\text{mod } p) \\
X_0^2 + Y_0^2 &\equiv 0(\text{mod } p).
\end{aligned}$$

As $p|(X_0^2 + Y_0^2)$, $X_0^2 + Y_0^2 = kp$, where $k \geq 1$. But $0 < |X_0|, |Y_0| < \sqrt{p}$. So, $X_0^2 + Y_0^2 < 2p$, implies that $k = 1$. QED.

1.1.6 Computation of Fermat's Two Square

The proof of *Fermat's two-square* theorem depends on *Thue's Lemma* and the square-root of -1 modulo the prime p which is of the form $4k + 1$. The proof of *Theu's Lemma* depends on *pigeon-hole principle*, and in that form it is not computable.
But we can us the *extended GCD* algorithm to compute (X_0, Y_0) as a solution of $ax \equiv y(\text{mod } p)$. Consider the following is the sequence of remainders $r_i,\ i = 0, \cdots, k, k + 1$, and Bezout's coefficients $x_i, y_i,\ i = 0, \cdots, k$, computed by the *extended GCD* algorithm.

$$(r_0 = p, 1, 0), (r_1 = a, 0, 1), \cdots, (r_i, x_i, y_i) \cdots (r_k, x_k, y_k),$$

where $r_{k+1} = 0$. As $gcd(p, a) = r_k = 1 = px_k + ay_k$. In general $r_i = px_i + ay_i$. The computation steps are as usual.

$$\begin{aligned}
r_{i-1} &= r_iq_i + r_{i+1}, \\
x_{i+1} &= x_{i-1} - x_iq_i, \\
y_{i+1} &= y_{i-1} - y_iq_i,\ \ i = 1, \cdots, k.
\end{aligned}$$

We continue the computation as long as $r_i \geq \sqrt{p}$ and stop at $r_i < \sqrt{p}$. This is possible as $r_0 = p > 0 = r_{k+1}$. On termination we set $Y_0 = r_i$ and $X_0 = y_i$. We know that $r_i = x_ip + y_ia$ i.e. $Y_0 = x_ip + X_0a$, so we have $aX_0 \equiv Y_0(\text{mod } n)$ where $0 < Y_0 < \sqrt{p}$.
We prove that $0 < |X_0| < \sqrt{p}$. Consider following two equations.

$$r_{i-1} = px_{i-1} + ay_{i-1}, \tag{1}$$
$$r_i = px_i + ay_i. \tag{2}$$

$(1)\times y_i-$ $(2)\times y_{i-1}$ gives us,

$$\begin{aligned} p(x_{i-1}y_i - x_iy_{i-1}) &= y_ir_{i-1} - y_{i-1}r_i \\ p \times (-1)^{i-1} &= y_ir_{i-1} - y_{i-1}r_i \\ p &= |y_ir_{i-1} - y_{i-1}r_i| \\ &= |y_i|r_{i-1} + |y_{i-1}|r_i,\ y_iy_{i-1} \leq 0, \\ &\quad y_i \text{ and } y_{i-1} \text{ have opposite signs.} \\ &\geq |y_i|r_{i-1}. \end{aligned}$$

We can prove by induction that $x_{i-1}y_i - x_iy_{i-1} = (-1)^{i-1}$. So,

$$|X_0| = |y_i| \leq \frac{p}{r_{i-1}} < \frac{p}{r_i} = \frac{p}{\sqrt{p}} = \sqrt{p}.$$

Example 8. Let $p = 83$, $a = 34$, $\lfloor\sqrt{83}\rfloor = 9$ So it Following is the table for *extended GCD* computation.

i	r_i	x_i	y_i	q_i
0	83	1	0	$-$
1	34	0	1	2
2	15	1	-2	2
3	4	-2	5	

So we have $Y_0 = r_3 = 4$ and $X_0 = y_3 = 5$ such that $0 < X_0, Y_0 < \sqrt{83}$. We have $83 \times (-2) + 34 \times 5 = 4$. A solution of $34x \equiv y (\text{mod } 83)$.

Now we turn our attention to the computation of the square-root of -1 modulo prime $p \equiv 1(\text{mod } 4)$. We want to compute an element $a \in \mathbb{Z}_p^*$ so that $a^2 \equiv -1(\text{mod } p)$. If we can find an element $b \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$, we may take $a = b^{\frac{p-1}{4}}$, as $a^2 \equiv (b^{\frac{p-1}{4}})^2 = b^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$ (Euler's criterion).

We know that half of the elements of $\mathbb{Z}_p^*$ are quadratic non-residue. So we can use the following randomised algorithm.

sqrt-1(p)
    `do`
        $b \leftarrow rand\{1, \cdots, p-1\}$
        $a \leftarrow b^{(p-1)/4}$
    `while` $(a^2 \text{ mod } p \neq p-1)$
    `return` a

The probability of picking a quadratic non-residue is $\frac{1}{2}$. So the expected number of times the loop is executed is 2. The probability that the algorithm has not found a quadratic non-residue after k iterations is $1/2^k$. The algorithm when terminates gives the correct a. But its running time is a *random variable* that is bounded. This type of algorithms are known as *Las Vegas algorithm*.

Modular exponentiation is the costly part of computation and we have seen that it takes $O(\log n)^3)$ time.

We are now ready to express a prime $p \equiv 1(\text{ mod } 4)$ as a sum of two squares in the following way. The input is p, where $p \equiv 1(\text{mod } 4)$

1. Find $a \in \mathbb{Z}_p^*$ such that $a^2 \equiv -1(\text{mod } p)$.
2. Take a and run the modified extended-GCD algorithm to compute (X_0, Y_0).

Example 9. Let $p = 977 = 4 \times 244 + 1$. Take $19 \in \mathbb{Z}_{977}^* \setminus (\mathbb{Z}_{977}^*)^2$ so that $19^{(977-1)/4} \equiv 725(\text{mod } 977)$ and $725^2 \equiv 976(\text{mod } 977)$. We have $\sqrt{977} > 31$. The run of the extended GCD algorithm on (p, a) is as follows:

i	r_i	x_i	y_i	q_i
0	977	1	0	$-$
1	725	0	1	1
2	252	1	-1	2
3	221	-2	3	1
4	31	3	-4	$\cdots$

At this point we stop computation where $Y_0 = 31$ and $X_0 = -4$. We express $977 = Y_0^2 + X_0^2 = 31^2 + 4^2$.

Proposition 20. A prime $p \equiv 1(\text{mod } 4)$ can be represented uniquely as a sum of two squares (ignoring sign and order).

Proof: Let $p = a^2 + b^2 = c^2 + d^2$. We rewrite it as

$$a^2d^2 + b^2d^2 - b^2c^2 - b^2d^2 = (a^2 + b^2)d^2 - (c^2 + d^2)b^2 = p(d^2 - b^2) \equiv 0(\text{mod } p).$$

So we have $(ad)^2 - (bc)^2 \equiv 0(\text{mod } p)$ i.e. $(ad + bc) \equiv 0(\text{mod } p)$ or $(ad - bc) \equiv 0(\text{mod } p)$. But we know that $a, b, c, d < \sqrt{p}$. So there are two possibilities either (i) $ad - bc = 0$, or (ii) $ad + bc = p$.

The second condition gives us

$$p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2.$$

It is equivalent to $ac = bd$.

We have two conditions (i) $ad - bc = 0$, or (ii) $ac = bd$.

If we consider the first condition $ad = bc$. We know that $gcd(a, b) = 1$, as p is prime. So $a|c$ i.e. $c = ak$ and we get $ad = kab$ implies that $d = kb$.

But then $p = c^2 + d^2 = k^2(a^2 + b^2)$ and p is prime. So $k = 1$, which implies that $a = c$ and $b = d$.

Similarly from the other condition we get the same result. QED.

Proposition 21. If n be a positive integer written as $n = N^2m$, where m is square free, then n can be represented as sum of two squares if and only if m does not contain a prime factor of the form $4k + 3$.

Proof: Let m has no prime factor of the form $4k+3$: if $m = 1$, then $n = N^2+0^2$. If $m = p_1 \cdots p_k$, where p_i is either 2 or any prime of the form $4k + 1$. So each $p_i = a_i^2 + b_i^2$. Given two such primes p_i and p_j we have

$$p_ip_j = (a_i^2 + b_i^2)(a_j^2 + b_j^2) = (a_ia_j + b_ib_j)^2 + (a_ib_j - b_ia_j)^2.$$

So by induction we can prove that m can be expressed as $a^2 + b^2$. And finally $n = (aN)^2 + (bN)^2$.

Let $n = N^2m$ can be written as $a^2 + b^2$. If $m = 1$, there is nothing to prove. Let $m > 1$ and also let $gcd(a, b) = d$, $a = dA$, $b = dB$. We have

$$a^2 + b^2 = d^2(A^2 + B^2) = n = N^2m.$$

m is square free so $d^2|N^2$. So we have

$$A^2 + B^2 = \frac{N^2}{d^2}m = qp,$$

where p is an odd prime factor of m. So,

$$A^2 + B^2 \equiv 0(\text{mod } p).$$

As $gcd(A, B) = 1$, either A or B is relatively prime to p. Otherwise p will divide both of them and the $gcd(A, B) \geq p$, a contradiction.

Let A be relatively prime to p. So we have

$$AA' \equiv 1(\text{mod } p)$$

So we have $(A^2 + B^2)(A')^2 \equiv 0(\text{mod } p)$, implies that $(AA')^2 + (BA')^2 \equiv 1 + (BA')^2 \equiv 0(\text{mod } p)$. So -1 is a quadratic residue of p implies that $p \equiv 1(\text{mod } 4)$. QED.

Proposition 22. A positive integer can be represented as a sum of two squares if and only if its prime factors of the form $4k + 3$ occurs in even power.

References

[AD] *Computational Number Theory* by Abhijit Das, Pub. CRC Press, 2013, ISBN 978-1-4398-6615-3.

[MD] *Primality Testing in Polynomial Time From Randomized Algorithms to "PRIMES is in P"*, by Martin Dietzfelbinger, LNCS 3000 (Tutorial), Pub. Springer, 2004, ISBN 3540403442.

[VS] *A Computational Introduction to Number Theory and Algebra* by Victor Shoup, 2nd ed., Pub. Cambridge University Press, 2009, ISBN 978-0-521-51644-0.

[EBV] *A Course in Algebra* by E B Vinberg, Graduate Studies in Mathematics, vol. 56, Pub. American Mathematical Society (Universities Press 2009), ISBN 978-0-8218-4858-6.