

Supplement to Chapter 2

These notes supplement Chapter 2 of the text. They develop more fully the implications of the Chinese remainder theorem, and illustrate the basic theory of quadratic residues.

1 The Chinese remainder map

In the proof of Theorem 2.12, we introduced the **Chinese remainder map**. Here, we present this map in more general terms, and list several important properties.

Theorem 1 (Chinese remainder map). *Let n_1, \dots, n_k be pairwise relatively prime, positive integers, and let $n := n_1 \cdots n_k$. Define the map*

$$\begin{aligned} \rho: \mathbb{Z}_n &\rightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [a]_n &\mapsto ([a]_{n_1}, \dots, [a]_{n_k}) \end{aligned}$$

(i) *The definition of ρ is unambiguous.*

(ii) *ρ is bijective.*

(iii) *Let $\alpha, \beta \in \mathbb{Z}_n$, with $\rho(\alpha) = (\alpha_1, \dots, \alpha_k)$ and $\rho(\beta) = (\beta_1, \dots, \beta_k)$. Then:*

$$\begin{aligned} \rho(\alpha + \beta) &= (\alpha_1 + \beta_1, \dots, \alpha_k + \beta_k), \\ \rho(\alpha\beta) &= (\alpha_1\beta_1, \dots, \alpha_k\beta_k). \end{aligned}$$

(iv) *Let $\alpha \in \mathbb{Z}_n$, with $\rho(\alpha) = (\alpha_1, \dots, \alpha_k)$. Then $\alpha \in \mathbb{Z}_n^*$ if and only if $\alpha_i \in \mathbb{Z}_{n_i}^*$ for $i = 1, \dots, k$, in which case*

$$\rho(\alpha^{-1}) = (\alpha_1^{-1}, \dots, \alpha_k^{-1}).$$

In particular, the restriction of ρ to \mathbb{Z}_n^ gives a one-to-one correspondence between \mathbb{Z}_n^* and $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.*

Proof. For (i), note that $a \equiv a' \pmod{n}$ implies $a \equiv a' \pmod{n_i}$ for $i = 1, \dots, k$, and so the definition of ρ is unambiguous (it does not depend on the choice of a).

(ii) follows directly from the statement of the Chinese remainder theorem.

(iii) follows easily from the rules of residue class arithmetic. Let $\alpha = [a]_n$ and $\beta = [b]_n$. Then $\alpha + \beta = [a + b]_n$, and so $\rho(\alpha + \beta) = ([a + b]_n, \dots, [a + b]_n)$. Moreover, for $i = 1, \dots, k$, we have $\alpha_i = [a]_{n_i}$ and $\beta_i = [b]_{n_i}$, and so $\alpha_i + \beta_i = [a + b]_{n_i}$. That proves the first identity; the other follows by similar reasoning.

For (iv), let α be as given, and let $\beta \in \mathbb{Z}_n$ with $\rho(\beta) = (\beta_1, \dots, \beta_k)$. Then since $\rho(\alpha\beta) = (\alpha_1\beta_1, \dots, \alpha_k\beta_k)$, we have $\alpha\beta = [1]_n$ if and only if $\alpha_i\beta_i = [1]_{n_i}$. \square

2 Quadratic Residues

Let n be a positive integer. An integer a is called a **quadratic residue modulo n** if $\gcd(a, n) = 1$ and $a \equiv b^2 \pmod{n}$ for some integer b ; in this case, we say that b is a **square root of a modulo n** . In terms of residue classes, a is a quadratic residue modulo n if and only if $[a]_n \in (\mathbb{Z}_n^*)^2$, where

$$(\mathbb{Z}_n^*)^2 := \{\beta^2 : \beta \in \mathbb{Z}_n^*\}$$

is the set of squares of elements of \mathbb{Z}_n^* . To avoid some annoying technicalities, we shall consider only the case where n is odd.

2.1 Quadratic residues modulo an odd prime

We begin our study of quadratic residues by considering the prime modulus case.

Theorem 2. *Let p be an odd prime and let $\alpha \in \mathbb{Z}_p$. Then $\alpha^2 = [1]$ if and only if $\alpha = \pm[1]$.*

Proof. Clearly, if $\alpha = \pm[1]$, then $\alpha^2 = [1]$. Conversely, suppose that $\alpha^2 = [1]$. Write $\alpha = [a]$ for $a \in \mathbb{Z}$. Then we have $a^2 \equiv 1 \pmod{p}$, which means that

$$p \mid (a^2 - 1) = (a - 1)(a + 1),$$

and since p is prime, we must have $p \mid (a - 1)$ or $p \mid (a + 1)$. This implies $a \equiv \pm 1 \pmod{p}$, or equivalently, $\alpha = \pm[1]$. \square

Theorem 3. *Let p be an odd prime and suppose $\alpha = \beta^2$ for some $\beta \in \mathbb{Z}_p^*$. Then for any $\gamma \in \mathbb{Z}_p^*$, we have $\alpha = \gamma^2$ if and only if $\gamma = \pm\beta$.*

Proof. Clearly, if $\gamma = \pm\beta$, then $\gamma^2 = \beta^2 = \alpha$. Conversely, if $\gamma^2 = \alpha$, then $(\gamma\beta^{-1})^2 = [1]$, and so by the previous theorem, $\gamma\beta^{-1} = \pm[1]$, and hence $\gamma = \pm\beta$. \square

Theorem 4. *Let p be an odd prime. Then $|(\mathbb{Z}_p^*)^2| = (p - 1)/2$.*

Proof. Note that for $\beta \in \mathbb{Z}_p^*$, β and $-\beta$ are distinct elements of \mathbb{Z}_p^* . By the previous theorem, the map $g : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ that sends β to β^2 is a two-to-one map: every element β^2 in the image of g has precisely two pre-images, namely, β and $-\beta$. It follows that the image of g is half the size of \mathbb{Z}_p^* . \square

Thus, for an odd prime p , exactly half the elements of \mathbb{Z}_p^* are squares, and half are non-squares. Indeed, we have

$$(\mathbb{Z}_p^*)^2 = \{[b]^2 : b = 1, \dots, (p - 1)/2\}.$$

To show this, it suffices to show that the integers b^2 , for $b = 1, \dots, (p - 1)/2$, lie in distinct residue classes modulo p . Let $b, c \in \{1, \dots, (p - 1)/2\}$, with $b^2 \equiv c^2 \pmod{p}$. We want to show that $b = c$. By Theorem 3, we have $b \equiv \pm c \pmod{p}$; that is, $p \mid (b + c)$ or $p \mid (b - c)$. However, since $0 < b + c < p$, we have $p \nmid (b + c)$, and so $p \mid (b - c)$; since $|b - c| < p$ and $b - c$ is a multiple of p , the only possibility is that $b = c$.

Example 1. Let $p = 7$. For $b = 1, \dots, 6$, we compute $b^2 \pmod{p}$:

$$1, 4, 2, 2, 4, 1.$$

Thus, the quadratic residues modulo 7 are 1, 4 and 2, which are congruent to the squares modulo 7 of 1, 2, and 3.

We next state an extremely important characterization of quadratic residues.

Theorem 5 (Euler's criterion). *Let p be an odd prime and let $\alpha \in \mathbb{Z}_p^*$.*

- (i) $\alpha^{(p-1)/2} = \pm[1]$.
- (ii) *If $\alpha \in (\mathbb{Z}_p^*)^2$ then $\alpha^{(p-1)/2} = [1]$.*
- (iii) *If $\alpha \notin (\mathbb{Z}_p^*)^2$ then $\alpha^{(p-1)/2} = -[1]$.*

Proof. For (i), let $\gamma = \alpha^{(p-1)/2}$. By Euler's theorem (Theorem 2.15), we have

$$\gamma^2 = \alpha^{p-1} = [1],$$

and hence by Theorem 2, we have $\gamma = \pm[1]$.

For (ii), suppose that $\alpha = \beta^2$. Then again by Euler's theorem, we have

$$\alpha^{(p-1)/2} = (\beta^2)^{(p-1)/2} = \beta^{p-1} = [1].$$

For (iii), let $\alpha \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$. We study the product

$$\epsilon := \prod_{\beta \in \mathbb{Z}_p^*} \beta.$$

We shall show that, on the one hand, $\epsilon = \alpha^{(p-1)/2}$, while on the other hand, $\epsilon = -[1]$.

To show that $\epsilon = \alpha^{(p-1)/2}$, we group elements of \mathbb{Z}_p^* into pairs of elements whose product is α . More precisely, consider the collection \mathcal{C} of all pairs $\{\kappa, \lambda\}$ such that $\kappa, \lambda \in \mathbb{Z}_p^*$, $\kappa \neq \lambda$, and $\kappa\lambda = \alpha$. We claim that \mathcal{C} is a partition of \mathbb{Z}_p^* . To see this, note that for all $\beta \in \mathbb{Z}_p^*$, if we set $\kappa := \beta$ and $\lambda := \alpha\beta^{-1}$, then we have $\kappa\lambda = \alpha$; moreover, $\kappa \neq \lambda$, since $\kappa = \lambda$ would imply that $\beta^2 = \alpha$, contradicting the assumption that $\alpha \notin (\mathbb{Z}_p^*)^2$. Thus, every $\beta \in \mathbb{Z}_p^*$ belongs to some pair in \mathcal{C} ; moreover, it is easy to see that distinct pairs in \mathcal{C} are disjoint: if $\kappa\lambda = \alpha = \kappa'\lambda'$ and $\kappa = \kappa'$, then $\lambda = \lambda'$. That proves the claim, from which it follows that

$$\epsilon = \prod_{\{\kappa, \lambda\} \in \mathcal{C}} (\kappa \cdot \lambda) = \prod_{\{\kappa, \lambda\} \in \mathcal{C}} \alpha = \alpha^{(p-1)/2}.$$

To show that $\epsilon = -[1]$, we group elements of \mathbb{Z}_p^* into pairs of elements whose product is $[1]$. More precisely, consider the collection \mathcal{D} of all pairs $\{\kappa, \lambda\}$ such that $\kappa, \lambda \in \mathbb{Z}_p^*$, $\kappa \neq \lambda$, and $\kappa\lambda = [1]$. We claim that \mathcal{D} is a partition of $\mathbb{Z}_p^* \setminus \{\pm[1]\}$. To see this, note that for all $\beta \in \mathbb{Z}_p^* \setminus \{\pm[1]\}$, if we set $\kappa := \beta$ and $\lambda := \beta^{-1}$, then we have $\kappa\lambda = [1]$; moreover, $\kappa \neq \lambda$, since $\kappa = \lambda$ would imply that $\beta^2 = [1]$, and Theorem 2 would imply that $\beta = \pm[1]$. Thus, every $\beta \in \mathbb{Z}_p^* \setminus \{\pm[1]\}$ belongs to some pair in \mathcal{D} ; conversely, if $\{\kappa, \lambda\} \in \mathcal{D}$, then neither

κ nor λ can be $\pm[1]$; moreover, it is also clear that distinct pairs in \mathcal{D} are disjoint. That proves the claim, from which it follows that

$$\epsilon = [1] \cdot (-[1]) \cdot \prod_{\{\kappa, \lambda\} \in \mathcal{D}} (\kappa \cdot \lambda) = - \prod_{\{\kappa, \lambda\} \in \mathcal{D}} [1] = -[1].$$

□

Euler's criterion provides a particularly simple way to determine modulo which primes -1 is a quadratic residue. Note that for an odd prime p , either $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

Theorem 6. *Let p be an odd prime. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$.*

Proof. By Euler's criterion, -1 is a quadratic residue modulo p if and only if $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. If $p \equiv 1 \pmod{4}$, then $(p-1)/2$ is even, and so $(-1)^{(p-1)/2} = 1$. If $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is odd, and so $(-1)^{(p-1)/2} = -1$. □

In fact, when $p \equiv 1 \pmod{4}$, any non-square in \mathbb{Z}_p^* yields a square root of -1 modulo p , as follows:

Theorem 7. *Let p be a prime with $p \equiv 1 \pmod{4}$, and let $\alpha \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$. Set $\omega := \alpha^{(p-1)/4}$. Then $\omega^2 = -[1]$.*

Proof. This is a simple calculation, based on Euler's criterion:

$$\omega^2 = \alpha^{(p-1)/2} = -[1].$$

□

The fact that -1 is a quadratic residue modulo primes $p \equiv 1 \pmod{4}$ can be used to prove Fermat's theorem that such primes may be written as the sum of two squares. To do this, we first need the following technical lemma:

Theorem 8 (Thue's lemma). *Let n, r^*, t^* be positive integers such that $r^* \leq n$ and $r^* t^* > n$, and let y be any integer. Then there exist integers r, t with*

$$ty \equiv r \pmod{n}, \quad |r| < r^*, \quad \text{and} \quad 0 < |t| < t^*.$$

Proof. For $i = 0, \dots, r^* - 1$ and $j = 0, \dots, t^* - 1$, define $v_{ij} := jy - i$. Since $r^* t^* > n$, two of the $r^* t^*$ values v_{ij} must lie in the same residue class modulo n ; that is, for some $(i_1, j_1) \neq (i_2, j_2)$, we have $v_{i_1 j_1} \equiv v_{i_2 j_2} \pmod{n}$. Setting $r := i_1 - i_2$ and $t := j_1 - j_2$, this implies $|r| < r^*$, $|t| < t^*$, and $ty \equiv r \pmod{n}$. It only remains to show that $t \neq 0$. However, $t = 0$ would imply $r \equiv 0 \pmod{n}$; however, since $(i_1, j_1) \neq (i_2, j_2)$, this would imply $r \neq 0$, and so r is a non-zero multiple of n ; in particular, $|r| \geq n \geq r^* > |r|$, a contradiction. □

Theorem 9 (Fermat's two squares theorem). *Let p be an odd prime. Then $p = r^2 + t^2$ for some integers r, t if and only if $p \equiv 1 \pmod{4}$.*

Proof. One direction is easy. Suppose $p \equiv 3 \pmod{4}$. Since the square of any integer is congruent to either 0 or 1 modulo 4 (verify), the sum of two squares is congruent to either 0, 1, or 2 modulo 4, and so can not be congruent to p modulo 4 (let alone equal to p).

For the other direction, suppose $p \equiv 1 \pmod{4}$. Then we know -1 is a quadratic residue modulo p ; that is, $y^2 \equiv -1 \pmod{p}$ for some integer y . Now apply Theorem 8 with $n := p$ and $r^* := t^* := \lfloor \sqrt{p} \rfloor + 1$. Evidently, $\lfloor \sqrt{p} \rfloor + 1 > \sqrt{p}$, and hence $r^*t^* > p$. Moreover, since p is prime, \sqrt{p} is not an integer, and so $\lfloor \sqrt{p} \rfloor < \sqrt{p}$; in particular, $\lfloor \sqrt{p} \rfloor + 1 \leq p$. Thus, the hypotheses of that theorem are satisfied, and therefore, there exist integers r and t such that

$$ty \equiv r \pmod{p}, \quad |r| < \sqrt{p}, \quad \text{and} \quad 0 < |t| < \sqrt{p}.$$

It follows that

$$r^2 \equiv t^2 y^2 \equiv -t^2 \pmod{p}.$$

Thus, $r^2 + t^2$ is a multiple of p and $0 < r^2 + t^2 < 2p$. The only possibility is that $r^2 + t^2 = p$. \square

2.2 Quadratic residues modulo an odd prime power

We now develop the basic theory of quadratic residues in the case where the modulus is of the form p^e , where p is an odd prime. The key to this is to establish the analog of Theorem 2:

Theorem 10. *Let p be an odd prime, e a positive integer, and let $\alpha \in \mathbb{Z}_{p^e}$. Then $\alpha^2 = [1]$ if and only if $\alpha = \pm[1]$.*

Proof. We have already proved this in the case $e = 1$, so assume $e > 1$. Clearly, if $\alpha = \pm[1]$, then $\alpha^2 = [1]$. Conversely, suppose that $\alpha^2 = [1]$. Write $\alpha = [a]$ for $a \in \mathbb{Z}$. We have $a^2 \equiv 1 \pmod{p^e}$, and we want to show that $a \equiv \pm 1 \pmod{p^e}$. Now, $a^2 \equiv 1 \pmod{p^e}$ implies $a^2 \equiv 1 \pmod{p}$, and so by Theorem 2, we have $a \equiv \pm 1 \pmod{p}$. If $a = \pm 1$, we are done, so assume that $a = \epsilon + p^f m$, where $\epsilon = \pm 1$, $m \in \mathbb{Z}$, $f > 0$, and $p \nmid m$. It will suffice to show that $f \geq e$. Suppose to the contrary that $f < e$. Then

$$a^2 = (\epsilon + p^f m)^2 = 1 + 2\epsilon p^f m + p^{2f} m^2.$$

So we have

$$0 \equiv a^2 - 1 \equiv 2\epsilon p^f m + p^{2f} m^2 \pmod{p^e},$$

which implies

$$0 \equiv 2\epsilon m + p^f m^2 \pmod{p^{e-f}},$$

and in particular (as $e > f$),

$$0 \equiv 2\epsilon m + p^f m^2 \equiv 2\epsilon m \pmod{p},$$

which is clearly impossible as $p \nmid 2\epsilon m$ (this is where we use in a critical way the fact that p is odd). \square

Theorems 3, 4, and 5 generalize immediately from \mathbb{Z}_p^* to $\mathbb{Z}_{p^e}^*$: we used nothing in the proofs of these theorems except for the fact that 1 has just two distinct square roots modulo p . As such, we state the analogs of these theorems for $\mathbb{Z}_{p^e}^*$ without proof.

Theorem 11. Let p be an odd prime and e a positive integer, and suppose $\alpha = \beta^2$ for some $\beta \in \mathbb{Z}_{p^e}^*$. Then for any $\gamma \in \mathbb{Z}_{p^e}^*$, we have $\alpha = \gamma^2$ if and only if $\gamma = \pm\beta$.

Theorem 12. Let p be an odd prime and e a positive integer. Then $|(\mathbb{Z}_{p^e}^*)^2| = \phi(p^e)/2$.

Theorem 13. Let p be an odd prime and e a positive integer, and let $\alpha \in \mathbb{Z}_{p^e}^*$.

(i) $\alpha^{\phi(p^e)/2} = \pm[1]$.

(ii) If $\alpha \in (\mathbb{Z}_{p^e}^*)^2$ then $\alpha^{\phi(p^e)/2} = [1]$.

(iii) If $\alpha \notin (\mathbb{Z}_{p^e}^*)^2$ then $\alpha^{\phi(p^e)/2} = -[1]$.

It turns out that an integer is a quadratic residue modulo p^e if and only if it is a quadratic residue modulo p .

Theorem 14. Let p be an odd prime and e a positive integer. Let a be an arbitrary integer. Then a is a quadratic residue modulo p^e if and only if a is a quadratic residue modulo p .

Proof. Suppose that a is a quadratic residue modulo p^e . Then a is not divisible by p and $a \equiv b^2 \pmod{p^e}$ for some integer b . It follows that $a \equiv b^2 \pmod{p}$, and so a is a quadratic residue modulo p .

Suppose that a is not a quadratic residue modulo p^e . If a is divisible by p , then by definition a is not a quadratic residue modulo p . So suppose a is not divisible by p . By Theorem 13, we have

$$a^{p^{e-1}(p-1)/2} \equiv -1 \pmod{p^e}.$$

This congruence holds modulo p as well, and by Fermat's little theorem (applied $e - 1$ times),

$$a \equiv a^p \equiv a^{p^2} \equiv \cdots \equiv a^{p^{e-1}} \pmod{p},$$

and so

$$-1 \equiv a^{p^{e-1}(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}.$$

Theorem 5 therefore implies that a is not a quadratic residue modulo p . □

2.3 Quadratic residues to an arbitrary odd modulus

Now we consider the theory of quadratic residues modulo an arbitrary, odd integer $n > 1$. Let

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

be the prime factorization of n . Our main tools here are the Chinese remainder map

$$\rho : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}},$$

discussed in Theorem 1, together with the results developed so far for quadratic residues modulo odd prime powers.

As usual, we begin by considering square roots of 1 modulo n . Let $\alpha \in \mathbb{Z}_n$ with $\rho(\alpha) = (\alpha_1, \dots, \alpha_r)$. Then since $\rho(\alpha^2) = (\alpha_1^2, \dots, \alpha_r^2)$, we have

$$\begin{aligned} \alpha^2 = [1] & \text{ iff } \alpha_i^2 = [1] \quad (i = 1, \dots, r) \\ & \text{ iff } \alpha_i = \pm[1] \quad (i = 1, \dots, r). \end{aligned}$$

Thus, if we let $U := \{\omega \in \mathbb{Z}_n : \omega^2 = [1]\}$, we see that U contains precisely 2^r elements, namely:

$$U = \rho^{-1}(\pm[1], \dots, \pm[1]).$$

Analogously to Theorem 3, if $\alpha = \beta^2$ for some $\beta \in \mathbb{Z}_n^*$, then $\gamma^2 = \alpha$ if and only if $\gamma = \omega\beta$ for some $\omega \in U$. Thus, each square in \mathbb{Z}_n^* has precisely 2^r square roots. Analogously to Theorem 4, since the squaring map on \mathbb{Z}_n^* is a 2^r -to-one mapping, we see that $|(\mathbb{Z}_n^*)^2| = \phi(n)/2^r$.

There is no natural analog of Euler's criterion in this case: the proof of that theorem relied critically on the fact that the only modular square roots of 1 were ± 1 .

The Chinese remainder map also allows to explicitly relate squares in \mathbb{Z}_n^* with squares in $\mathbb{Z}_{p_i}^{*e_i}$. Let $\alpha, \beta \in \mathbb{Z}_n^*$ with $\rho(\alpha) = (\alpha_1, \dots, \alpha_r)$ and $\rho(\beta) = (\beta_1, \dots, \beta_r)$. Then since $\rho(\beta^2) = (\beta_1^2, \dots, \beta_r^2)$, we have

$$\alpha = \beta^2 \text{ iff } \alpha_i = \beta_i^2 \quad (i = 1, \dots, r).$$

Thus, $\alpha \in \mathbb{Z}_n^*$ if and only if $\alpha \in (\mathbb{Z}_{p_i}^{*e_i})^2$ for $i = 1, \dots, r$; moreover, if $\alpha_i = \beta_i^2$, then the square roots of α are

$$\rho^{-1}(\pm\beta_1, \dots, \pm\beta_r).$$

EXERCISE 1. Let n be an arbitrary positive integer, and let $\alpha, \beta \in \mathbb{Z}_n^*$. Show that:

- (a) if $\alpha \in (\mathbb{Z}_n^*)^2$ and $\beta \in (\mathbb{Z}_n^*)^2$, then $\alpha\beta \in (\mathbb{Z}_n^*)^2$;
- (b) if $\alpha \in (\mathbb{Z}_n^*)^2$, then $\alpha^{-1} \in (\mathbb{Z}_n^*)^2$;
- (c) if $\alpha \in (\mathbb{Z}_n^*)^2$ and $\beta \notin (\mathbb{Z}_n^*)^2$, then $\alpha\beta \notin (\mathbb{Z}_n^*)^2$;
- (d) if n is an odd prime power, $\alpha \notin (\mathbb{Z}_n^*)^2$, and $\beta \notin (\mathbb{Z}_n^*)^2$, then $\alpha\beta \in (\mathbb{Z}_n^*)^2$;
- (e) the assumption that n is an odd prime power is necessary in part (d) by giving an explicit example where it fails without this assumption.

EXERCISE 2. Let p be a prime with $p \equiv 1 \pmod{4}$. Let $a := ((p-1)/2)!$. Show that $a^2 \equiv -1 \pmod{p}$.

EXERCISE 3. Let n be a positive integer, and write $n = m^2\ell$ where m and ℓ are integers and ℓ is square-free (see Exercise 1.13 in the text). Show that n is the sum of two squares of integer if and only if no prime $p \equiv 3 \pmod{4}$ divides ℓ .