Chapter 6

Quadratic Residues

The very structural theory of congruences we have built thus far leads us to the next level: quadratic congruences. The existence question of square roots modulo a prime will be consummated in the celebrated law of quadratic reciprocity. Our approach toward this goal will follow closely that of the text [NZM91]. Meanwhile, actual algorithms needed to solve quadratic congruences will be treated only briefly in this chapter, but to be continued and settled in Appendix D.

6.1 Quadratic Residues and Nonresidues

The simplest quadratic congruence will be $x^2 \equiv a \pmod{n}$. We shall first differentiate between the values of a for which this congruence has a solution and those for which it does not.

Definition. A number a which is relatively prime to n is a *quadratic residue* modulo n if the congruence $x^2 \equiv a \pmod{n}$ has a solution. If it has no solution, then a is called a *quadratic nonresidue* modulo n. For example, 19 is a quadratic residue modulo 5 since $19 \equiv 2^2 \pmod{5}$, but 7 is a nonresidue because there is no integer whose square belongs to $[7]_5$.

It is clear that being a quadratic residue, or nonresidue, is a characteristic of the entire residue class of a modulo n. Hence, as usual, we will use the phrase *distinct* or *incongruent* quadratic (non)residues when we mean that they belong to different residue classes.

Moreover, the solutions to $x^2 \equiv a \pmod{n}$, if any, are also given by residue classes. In particular, the task of separating the quadratic residues from the nonresidues can be done within a chosen reduced residue system.

For example, modulo 14 we look at $\{1, 3, 5, 9, 11, 13\}$. We have

$$\begin{array}{llllll} 1^2 \equiv 1 & \pmod{14} & 3^2 \equiv 9 & \pmod{14} & 5^2 \equiv 11 & \pmod{14} \\ 9^2 \equiv 11 & \pmod{14} & 11^2 \equiv 9 & \pmod{14} & 13^2 \equiv 1 & \pmod{14} \end{array}$$

The quadratic residues modulo 14 are therefore given by [1], [9], and [11], whereas quadratic nonresidues by [3], [5], and [13].

Exercise 6.1. Find all the quadratic residues and nonresidues modulo n.

a) $n = 8$
b) $n = 9$
c) $n = 10$
d) $n = 11$
e) $n = 12$

Exercise 6.2. Unlike primitive roots, show that quadratic nonresidues exist with any modulus $n > 2$. (So do quadratic residues, e.g., $a = 1$.)

Exercise 6.3. Suppose g is a primitive root modulo $n > 2$.

a) Show that g^k is a quadratic residue modulo n if and only if k is even. In particular, it follows that every primitive root is a quadratic nonresidue.
b) Prove there are as many quadratic residues as nonresidues modulo n.
c) Give an example where (b) is false when modulo n has no primitive roots.
d) Prove that the product ab is a quadratic residue modulo n if and only if either both a and b are quadratic residues or both nonresidues.

The Chinese remainder theorem allows us to eventually reduce the congruence $x^2 \equiv a \pmod{n}$, or any congruence, to the case where n is a prime power. Our next focus will be on prime modulus, with which the terms quadratic residue and nonresidue can then be numerically denoted by the Legendre symbol, a very convenient as well as useful notation.

Definition. The *Legendre symbol* is written and defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{if } p \mid a \end{cases}$$

for any integer a and prime $p > 2$. Some authors prefer the notation $(a|p)$ for the Legendre symbol. We shall use both interchangeably, mainly for the sake of readability—the vertical mode in a displayed equation and the horizontal mode for intext. For example, we have earlier seen that $(19|5) = 1$ and $(7|5) = -1$. Note also that $(a|p) = (b|p)$ whenever $a \equiv b \pmod{p}$ and, in particular,

$$\left(\frac{a}{p}\right) = \left(\frac{a \,\%\, p}{p}\right)$$

Exercise 6.4. Investigate true or false.

a) $(a|p) = (b|p)$ implies $a \equiv b \,(\operatorname{mod} p)$
b) $(1|p) = 1$
c) $(-1|p) = -1$
d) $(a^2|p) = (a|p)^2$

We shall henceforth agree that the number p in the notation $(a|p)$ is always understood an odd prime, i.e., a prime $p > 2$. With that, the next *Euler's criterion* states a very useful congruence for the Legendre symbol.

Theorem 6.1 (Euler's Criterion)**.** The Legendre symbol $(a|p)$ satisfies

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

Proof. It is trivial if $p \mid a$, else apply Corollary 5.9 with $k = 2$. ▽

Exercise 6.5. Alternately, prove Theorem 6.1 using Exercise 6.3(a).

Corollary 6.2. The following equalities hold for the Legendre symbol.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{and} \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

Proof. Assume $p \nmid ab$ to avoid triviality. In each equation, left and right are congruent modulo $p > 2$, by Theorem 6.1. But each quantity is ± 1; the only way this can happen is when both sides are 1 or both -1. ▽

Note that the second equality gives $(-1|p) = 1$ if $p \,\%\, 4 = 1$, and $(-1|p) = -1$ if $p \,\%\, 4 = 3$. This result agrees with that given earlier in Exercise 5.22.

Example. Let us apply the above properties in evaluating $(-75|17)$. We have $(-75|17) = (-1|17)(5|17)^2(3|17) = (-1)^8(\pm 1)^2(3|17) = (3|17)$. And then $(3|17) \equiv 3^8 \,(\operatorname{mod} 17)$ according to Euler's criterion (Theorem 6.1). Successive squaring algorithm gives us $3^8 \,\%\, 17 = 16$, hence $(-75|17) = -1$.

There really are different ways to arrive at this same result. For instance, since $-75 \equiv 27 \,(\operatorname{mod} 17)$ then $(-75|17) = (27|17) = (3|17)^3 = (3|17)$. Or by the fact that $-75 \,\%\, 17 = 10$, we have $(-75|17) = (10|17) = (2|17)(5|17)$. Or Euler's criterion alone, $(10|17) \equiv 10^8 \,(\operatorname{mod} 17)$, etc.

Exercise 6.6. Evaluate the Legendre symbol $(a|p)$ in several ways.

a) $(-35|11)$
b) $(54|13)$
c) $(-28|19)$
d) $(11|23)$

Exercise 6.7. Let p be an odd prime relatively prime to a. Prove that the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ has a solution if and only if $(b^2 - 4ac|p) \geq 0$. Then determine the solvability of the following.
a) $x^2 \equiv -1 \pmod{101}$
b) $x^2 - 5x + 2 \equiv 0 \pmod{29}$
c) $2x^2 \equiv 18x + 24 \pmod{43}$
d) $13x^2 - 56x \equiv 44 \pmod{79}$

As a matter of fact, there are yet other ways by which we can evaluate the Legendre symbol. The next two lemmas are not that practical, but they carry some theoretical significance. The first of the two is that of Gauss.

Lemma 6.3 (Gauss's Lemma)**.** Consider the Legendre symbol $(a|p)$ with $p \nmid a$. Let $d = (p-1)/2$ and $A = \{a, 2a, 3a, \ldots, da\}$. Then $(a|p) = (-1)^n$, where n is the number of elements $x \in A$ such that $x \,\%\, p > d$.

Proof. Since $p \nmid a$, elements of A are distinct modulo p. Now consider the reduced residue system modulo p given by $S = \{\pm 1, \pm 2, \ldots, \pm d\}$. Note that the solutions to $x \,\%\, p > d$ in S are precisely given by the negative elements,[1] exactly n of which are congruent to an element in A.

In S, only one number in each plus/minus pair can be congruent modulo p to some element in A. If this claim were false, we would have $ia, ja \in A$, with $1 \leq i < j \leq d$, for which $ia \equiv -ja \pmod{p}$, and so $i \equiv -j \pmod{p}$. This is impossible as both i and $-j$ belong to S, a reduced residue system.

It follows that, modulo p, the elements of A are reordering of the numbers 1, 2, ... , d—only that n of them are prefixed by the negative sign. Then,

$$a \times 2a \times \cdots \times da \;\equiv\; (-1)^n \times 1 \times 2 \times \cdots \times d \pmod{p}$$

from which we claim $(-1)^n \equiv a^d \equiv (a|p) \pmod{p}$, by Euler's criterion. ▽

Example. Let us illustrate Gauss's lemma with $a = 5$ and $p = 17$, hence $d = 8$. We have $A = \{5, 10, 15, 20, 25, 30, 35, 40\}$, reduced mod 17 to $\{5, 10, 15, 3, 8, 13, 1, 6\}$. Three elements exceed 8, so $(5|17) = (-1)^3 = -1$.

Exercise 6.8. Redo Exercise 6.6 using Gauss's lemma.

At this point we are able to derive the following formula for $(2|p)$, a special case of the Legendre symbol which will be encountered quite frequently in computation.

Proposition 6.4. The following formula holds for $(2|p)$.

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

[1] In fact, $x \,\%\, p > d$ if and only if $x \,\%\%\, p < 0$. See Exercise 1.8 for definition.

Proof. We claim, as an easy exercise, that the exponent $(p^2-1)/8$ is even if and only if $p \equiv \pm 1 \pmod 8$.

Let us keep the same notation we use in Lemma 6.3 and its proof. We repeat that elements of A are congruent modulo p to 1, 2, ... , d, not necessarily in this order, except that n of them should have the negative sign. Denote by r_i's those which should have been negative, and the rest by s_j's. Then, for $1 \le k \le d$, the residue $ka \,\%\, p$ is either s_j or $p - r_i$ for some indices i and j. Using the relation $ka = \lfloor \frac{ka}{p} \rfloor p + ka \,\%\, p$, we take sums over k,

$$\sum_{k=1}^{d} ka = \sum_{k=1}^{d} \left\lfloor \frac{ka}{p} \right\rfloor p + \sum_{i=1}^{n} p - r_i + \sum_{j=1}^{d-n} s_j \tag{6.1}$$

On the other hand, we also have

$$\sum_{k=1}^{d} k = \sum_{i=1}^{n} r_i + \sum_{j=1}^{d-n} s_j \tag{6.2}$$

Next, we subtract Equation 6.2 from Equation 6.1, to get

$$(a-1)\sum_{k=1}^{d} k = \sum_{k=1}^{d} \left\lfloor \frac{ka}{p} \right\rfloor p + \sum_{i=1}^{n} p - 2\sum_{i=1}^{n} r_i \tag{6.3}$$

If we now let $a = 2$, then $\lfloor \frac{2k}{p} \rfloor = 0$ since $2k < p$, and Equation 6.3 becomes $d(d+1)/2 = np - 2\sum r_i$. As p is odd, this quantity is even or odd as n is. By Lemma 6.3, then $(2|p) = (-1)^n = (-1)^{d(d+1)/2}$. Substitute $d = (p-1)/2$, and we are done. ▽

Exercise 6.9. Complete the proof that $(2|p) = 1$ if and only if $p \in [\pm 1]_8$. Similarly, show that $(-2|p) = 1$ if and only if $p \,\%\, 8 = 1$ or 3.

The second lemma, due to Eisenstein, is to be proved along the same line. We will need Eisenstein's lemma mainly in proving the law of quadratic reciprocity, the coming paramount theorem for the Legendre symbol.

Lemma 6.5 (Eisenstein's Lemma)**.** If $p \nmid a$, and both are odd, then

$$\left(\frac{a}{p}\right) = (-1)^m \quad \text{where} \quad m = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor$$

Proof. As $a \equiv p \equiv 1 \pmod 2$, this time Equation (6.3) gives the congruence $0 \equiv m + n \pmod 2$. Again, this means that m is of the same parity as that of the number n in Gauss's lemma, and hence $(-1)^m = (-1)^n = (a|p)$. ▽

Example. We illustrate Eisenstein's lemma with $a = 5$ and $p = 17$. We have

$$\begin{aligned} m &= \lfloor \tfrac{5}{17} \rfloor + \lfloor \tfrac{10}{17} \rfloor + \lfloor \tfrac{15}{17} \rfloor + \lfloor \tfrac{20}{17} \rfloor + \lfloor \tfrac{25}{17} \rfloor + \lfloor \tfrac{30}{17} \rfloor + \lfloor \tfrac{35}{17} \rfloor + \lfloor \tfrac{40}{17} \rfloor \\ &= 0 + 0 + 0 + 1 + 1 + 1 + 2 + 2 = 7 \end{aligned}$$

and $(5|17) = (-1)^7 = -1$.

Exercise 6.10. Redo Exercise 6.6 using Eisenstein's lemma.

At last we will now show that the Legendre symbol obeys a reciprocity law in which $(q|p)$, where q is another odd prime, may be replaced by $(p|q)$ according to the following rule.

Theorem 6.6 (The Law of Quadratic Reciprocity)**.** If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Proof. Consider all ordered pairs (x, y) with $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq q \leq \frac{q-1}{2}$. There are exactly $\frac{(p-1)}{2} \times \frac{(q-1)}{2}$ such elements, which can be grouped into two classes—in the first class if $py < qx$, and in the second if $py > qx$. Note that $py = qx$ is not possible since $p \nmid qx$. For each x, the condition $py < qx$ is equivalent to $1 \leq y \leq \lfloor \frac{qx}{p} \rfloor$, and hence the first class consists of m_1 elements, where $m_1 = \sum_{x=1}^{(p-1)/2} \lfloor \frac{qx}{p} \rfloor$. Similarly, $m_2 = \sum_{y=1}^{(q-1)/2} \lfloor \frac{py}{q} \rfloor$ for the second class. In all,

$$\frac{(p-1)(q-1)}{4} = m_1 + m_2 = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor$$

Hence $(-1)^{(p-1)(q-1)/4} = (-1)^{m_1}(-1)^{m_2} = (q|p)(p|q)$ by Lemma 6.5. ▽

Exercise 6.11. For any pair of odd primes p and q, show that $(q|p) = (p|q)$, except when both primes belong to the class $[3]_4$, for then $(q|p) = -(p|q)$.

Exercise 6.12. If $p \equiv \pm q \pmod{4a}$ then $(a|p) = (a|q)$. Prove that this fact, initially conjectured by Euler, is equivalent to Theorem 6.6.

Example. Consider $(4459|6247)$. The factorization $4459 = 7^3 \times 13$ enables us to write $(4459|6247) = (7|6247)(13|6247)$. The next steps consist of repeated applications of Theorem 6.6 and the replacement of $(a|p)$ by $(a \,\%\, p|p)$.

$$\left(\frac{7}{6247}\right) = -\left(\frac{6247}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{13}{6247}\right) = \left(\frac{6247}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^3 = -1$$

Putting the two together, we conclude that $(4459|6247) = -1$.

Exercise 6.13. Evaluate $(a|p)$ with the help of the reciprocity law.

a) $(37|83)$
b) $(71|103)$
c) $(-69|127)$
d) $(1414|2063)$
e) $(19392|2939)$

Exercise 6.14. Show that $(3|p) = 1$ if and only if $p \in [\pm 1]_{12}$. Similarly, $(-3|p) = 1$ if and only if $p \,\%\, 6 = 1$.

Exercise 6.15. Modulo which odd prime is 5 is a quadratic residue?

6.2 The Jacobi Symbol

Despite all the variety of tools we have for evaluating the Legendre symbol $(a|p)$, we just cannot avoid the need of factoring a. This slows down computation time a great deal, especially when p is large. The Jacobi symbol is an extension of the Legendre symbol in the way that the "denominator" can now be any odd number, not necessarily prime. This will make possible a very fast algorithm to compute $(a|p)$, almost in an analogous way that the Euclidean algorithm enables us to compute gcd without factoring.

Definition. Let $n = p_1 p_2 \cdots p_k$ be the product of odd prime numbers, not necessarily distinct. Define the *Jacobi symbol* $(a|n)$ by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

where each factor $(a|p_i)$ is the Legendre symbol. Moreover, let $(a|1) = 1$.

As an example, we have $(14|1275) = (14|3)(14|5)(14|5)(14|17)$ because $1275 = 3 \times 5^2 \times 17$. Note that if $\gcd(a,n) = 1$, then the value of $(a|n)$ is ± 1, and 0 otherwise. In addition, if $k = 1$ then the two symbols—Legendre and Jacobi—are one and the same. It is furthermore true that if $(a|n) = -1$, then a is a quadratic nonresidue modulo n, but the converse is sometimes false.

Exercise 6.16. Evaluate the Jacobi symbol $(14|1275)$. Is 14 a quadratic residue modulo 1275? Why or why not?

The Jacobi symbol too respects residue classes, for if $a \equiv b \pmod{n}$ then $a \equiv b \pmod{p_i}$ for each prime p_i dividing n, thus $(a|n) = \prod(a|p_i) = \prod(b|p_i) = (b|n)$. Surprisingly enough, the Jacobi symbol furthermore enjoys the main properties of the Legendre symbol given in the previous section, including the law of reciprocity.

Theorem 6.7. With the Jacobi symbol, for any odd number $n > 0$,

1) $(ab|n) = (a|n)(b|n)$

2) $(-1|n) = (-1)^{(n-1)/2}$

3) $(2|n) = (-1)^{(n^2-1)/8}$

4) $(m|n) = (n|m)(-1)^{(m-1)(n-1)/4}$ if m is also an odd positive number.

Proof. Let $n = \prod p_i$ with odd prime factors, not assumed distinct. The first equality holds as $(ab|n) = \prod(ab|p_i) = \prod(a|p_i)(b|p_i) = (a|n)(b|n)$.

Now for each factor, $(-1|p_i) = \pm 1$ if and only if $p_i \in [\pm 1]_4$, with plus or minus, respectively. (See Corollary 6.2 or Exercise 5.22.) Then, $(-1|n) = 1$ if and only if the case $p_i \in [-1]_4$ occurs an even number of times, which is equivalent to having $n \,\%\, 4 = 1$. This is the fact expressed in (2).

Similarly, by Proposition 6.4, $(2|p_i) = 1$ when $p_i \in [\pm 1]_8$, and $(2|p_i) = -1$ if $p_i \in [\pm 3]_8$. Note that for any pair $x, y \in [\pm 3]_8$, we have $xy \in [\pm 1]_8$. Therefore, $(2|n) = 1$ if and only if $n \equiv \pm 1 \pmod 8$, proving (3).

For (4), write $m = \prod q_j$ where, again, there may be repeated prime factors. Assume also that $\gcd(m, n) = 1$, or else $(m|n) = (n|m) = 0$. Then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod\prod\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod\prod (-1)^{(p_i-1)(q_j-1)/4}$$

This quantity is -1 if and only if there is an odd number of pairs (p_i, q_j) with both primes in the class $[-1]_4$ (Exercise 6.11). Equivalently, this occurs when both m and n each has an odd number of prime factors in this class, i.e., when $m \equiv n \equiv -1 \pmod 4$. Hence, $(m|n)(n|m) = (-1)^{(m-1)(n-1)/4}$. ▽

Example. We reconsider the evaluation of the Legendre symbol $(4459|6247)$, this time with the help of Jacobi symbols.

$$\begin{aligned}\left(\frac{4459}{6247}\right) &= -\left(\frac{6247}{4459}\right) = -\left(\frac{1788}{4459}\right) = -\left(\frac{2}{4459}\right)^2\left(\frac{447}{4459}\right) = \left(\frac{4459}{447}\right)\\ &= \left(\frac{436}{447}\right) = \left(\frac{2}{447}\right)^2\left(\frac{109}{447}\right) = \left(\frac{447}{109}\right) = \left(\frac{11}{109}\right) = \left(\frac{109}{11}\right)\\ &= \left(\frac{10}{109}\right) = \left(\frac{2}{109}\right)\left(\frac{5}{109}\right) = (-1)^{1485}\left(\frac{109}{5}\right) = -\left(\frac{4}{5}\right)\end{aligned}$$

The same conclusion, $(4459|6247) = -1$. But note that neither 4459 nor 447 is prime, and that the only factoring needed is for the even factors.

Exercise 6.17. Evaluate the Jacobi symbol $(1939|29391)$.

Exercise 6.18. Redo Exercise 6.13 with the help of Jacobi symbols.

Recall Exercise 6.3(b), which says that quadratic residues and nonresidues modulo $n > 2$ are equally many, provided that we have primitive roots. The next problem claims that the Jacobi symbol $(a|n)$ takes on the values ± 1 equally many times, if n has no repeated prime factors.

Exercise 6.19. Let n be the product of distinct odd primes.

a) Show that $(a|n) = -1$ for some a relatively prime to n.
b) Prove that $\sum (a_i|n) = 0$ over any reduced residue system modulo n.
c) Conclude that $(x|n) = \pm 1$ each has $\phi(n)/2$ incongruent solutions.
d) Find a counter-example for (c) where n is divisible by a square.

6.3 Extracting Square Roots

Having developed the tools to answer the existence question, we turn now to the actual problem of finding the modular square roots. If a is a quadratic residue modulo the odd prime p, then Corollary 5.9 says that the congruence $x^2 \equiv a \pmod{p}$ has exactly two solutions given by $[\pm x_0]_p$, for any particular solution x_0. Still, this knowledge does not readily reveal the value of x_0, except in the following special case.

Theorem 6.8. If $(a|p) = 1$ and $p \,\%\, 4 = 3$, then there are exactly two solutions to the congruence $x^2 \equiv a \pmod{p}$, given by $x \equiv \pm a^{(p+1)/4} \pmod{p}$.

Proof. By Euler's criterion, $(a^{(p+1)/4})^2 = a^{(p+1)/2} = a^{(p-1)/2} a \equiv a \pmod{p}$. That the two solutions are distinct is clear since $p \nmid 2a$, thus the theorem follows from Corollary 5.9. $\triangledown$

Example. Let us apply Theorem 6.8 to $x^2 \equiv 7 \pmod{19}$. We first verify that $(7|19) = -(19|7) = -(5|7) = -(7|5) = -(2|5) = 1$, and that $19 \,\%\, 4 = 3$. A particular solution is $x_0 = 7^{(19+1)/4} = 7^5 = 16807$. One solution class is given by $[16807]_{19} = [11]_{19}$, and the other by $[-11]_{19} = [8]_{19}$.

Exercise 6.20. Solve the following congruences.

a) $x^2 \equiv 2 \pmod{23}$
b) $x^2 \equiv 8 \pmod{83}$
c) $x^2 - 2x + 3 \equiv 0 \pmod{11}$
d) $2x^2 + x + 2 \equiv 0 \pmod{31}$

The case $p \,\%\, 4 = 1$ is generally rather complex, but half of the time, when $p \,\%\, 8 = 5$, it is yet manageable without needing special algorithms.

Theorem 6.9. Suppose that $(a|p) = 1$ and $p \,\%\, 8 = 5$. Let $r = a^{(p+3)/8}$. Then either r or $2^{(p-1)/4} \times r$ is a solution to the congruence $x^2 \equiv a \pmod{p}$.

Proof. In this case $(2|p) = -1$, (Proposition 6.4) so $2^{(p-1)/2} \equiv -1 \pmod{p}$ by Euler's criterion. And now, the congruence $r^4 = a^{(p-1)/2}a^2 \equiv a^2 \pmod{p}$ implies that $r^2 \equiv \pm a \pmod{p}$. (See Exercise 3.12.) If $r^2 \equiv -a \pmod{p}$, then $2^{(p-1)/4} \times r$ is a solution to $x^2 \equiv a \pmod{p}$. ▽

Example. Let us solve $x^2 \equiv 5 \pmod{29}$, noting that $29 \,\%\, 8 = 5$. We have here $r = 5^4 \,\%\, 29 = 16$. As we check, $16^2 \,\%\, 29 = 24 \equiv -5 \pmod{29}$, hence the multiplier $2^7 \,\%\, 29 = 12$ is needed. A particular solution is then $x_0 = 12 \times 16 = 192$, yielding the two classes of solution, $[\pm 192]_{29} = [\mp 11]_{29}$.

Exercise 6.21. Solve the congruence $x^2 \equiv 33 \pmod{101}$.

With the last theorem, the problem of extracting square roots modulo p is left to the case $p \,\%\, 8 = 1$. A complete treatment of this topic can be found in Appendix D. For now, instead, we demonstrate how one might find square roots modulo the product of two distinct primes.

Example. Solve the congruence $x^2 \equiv 54 \pmod{115}$, given that $115 = 5 \times 23$. By the Chinese remainder theorem, the congruence is equivalent to the pair below, whose solutions can each be found using Theorems 6.8 and 6.9.

$$\begin{array}{ccc} y^2 \equiv 54 \equiv 4 \pmod{5} & \leftrightarrow & y \equiv \pm 2 \pmod{5} \\ z^2 \equiv 54 \equiv 8 \pmod{23} & \leftrightarrow & z \equiv \pm 13 \pmod{23} \end{array}$$

And by the Chinese remainder theorem again, we conclude that there is a total of four distinct solutions modulo 115,

$$\begin{array}{ccccc} y \equiv +2 \pmod{5} & \text{and} & z \equiv +13 \pmod{23} & \leftrightarrow & x \equiv +82 \pmod{115} \\ y \equiv +2 \pmod{5} & \text{and} & z \equiv -13 \pmod{23} & \leftrightarrow & x \equiv -13 \pmod{115} \\ y \equiv -2 \pmod{5} & \text{and} & z \equiv +13 \pmod{23} & \leftrightarrow & x \equiv +13 \pmod{115} \\ y \equiv -2 \pmod{5} & \text{and} & z \equiv -13 \pmod{23} & \leftrightarrow & x \equiv -82 \pmod{115} \end{array}$$

Note that this divide-and-conquer technique clearly generalizes to any modulus which factors into three or more distinct primes.

Exercise 6.22. Solve these congruences, modulo $n = pq$.

a) $x^2 \equiv 10 \pmod{21}$
b) $x^2 \equiv 29 \pmod{35}$
c) $x^2 \equiv 31 \pmod{55}$
d) $x^2 \equiv 106 \pmod{119}$
e) $x^2 \equiv 102 \pmod{341}$

Exercise 6.23. Using the Chinese remainder theorem, show that if a is a quadratic residue modulo an odd composite n, then $x^2 \equiv a \pmod{n}$ has exactly 2^t incongruent solutions, where t is the number of distinct prime divisors of n. Then find all the solutions to $x^2 \equiv 1 \pmod{7425}$.

6.4 Electronic Coin Tossing [Project 6]

In a game of coin tossing, two players have a fifty-fifty chance of winning by betting on the outcome, either *head* or *tail.* How can this game be played electronically, over email for instance? This was answered in 1982 by M. Blum.

Alia selects two large primes p and q, both from the class $[3]_4$, and sends the product $n = pq$ to Bob. In turn, Bob chooses an integer $h < n$ and sends $a = h^2 \,\%\, n$ to Alia. Using Theorem 6.8 plus the Chinese remainder theorem, Alia is able to solve $x^2 \equiv a \pmod{n}$ and find the four square roots, in the forms $x_1 \equiv \pm h \pmod{n}$ and $x_2 \equiv \pm t \pmod{n}$.

Now Alia must guess Bob's number, either h or t. If Alia sends h to Bob, Alia wins. If, however, she bets on t then Bob wins, and he shall prove his victory by factoring n, which supposedly only Alia knows. How will Bob do it? Knowing both h and t, Bob simply computes $\gcd(h \pm t, n)$ in no time[2] using the Euclidean algorithm, and that will give him p and q.

Project 6.4.1. Justify each claim assumed in this protocol and illustrate it using your own numerical example. By the way, though not needed in this context, show that exactly one of the four numbers, $\pm h$ and $\pm t$, is a quadratic residue modulo n.

Project 6.4.2. Do a library or internet research on how to devise a similar protocol for playing poker over the telephone!

[2] Well, in at most $O(\log^2 n)$ time.