USING QUADRATIC RECIPROCITY (CTNT 2024)

KEITH CONRAD

1. Introduction

The quadratic reciprocity law says that when p and q are distinct odd primes

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\dfrac{p}{q}\right), & \text{if } p \text{ or } q \equiv 1 \bmod 4, \\ -\left(\dfrac{p}{q}\right), & \text{if } p \text{ and } q \equiv 3 \bmod 4 \end{cases} \tag{1.1}$$

and

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv 3 \bmod 4, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \bmod 8, \\ -1, & \text{if } p \equiv 3, 5 \bmod 8, \end{cases} \tag{1.2}$$

Equation (1.1) is called the *main law* of quadratic reciprocity and the equations in (1.2) are called the *supplementary laws*. In words, the main law says

- if p *or* q is 1 mod 4 then $q \equiv \square \bmod p$ if and only if $p \equiv \square \bmod q$,[1]
- if p *and* q are 3 mod 4 then $q \equiv \square \bmod p$ if and only if $p \not\equiv \square \bmod q$.

The supplementary laws say $-1 \equiv \square \bmod p$ if and only if $p \equiv 1 \bmod 4$ and $2 \equiv \square \bmod p$ if and only if $p \equiv \pm 1 \bmod 8$.

The equations in (1.1) and (1.2) are expressible without using cases as

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right), \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{1.3}$$

Proofs of quadratic reciprocity usually involve mysterious calculations. it is not any clearer why quadratic reciprocity should be true after you have read a proof than before you read the proof. Our goal here is not to prove quadratic reciprocity, but to use it.

2. Square patterns

Using quadratic reciprocity we can work out, for nonzero $a \in \mathbf{Z}$, a description of all odd primes p such that $(\frac{a}{p}) = 1$.

Example 2.1. Let's show for primes $p \neq 2$ that $(\frac{-2}{p}) = 1$ if and only if $p \equiv 1, 3 \bmod 8$.

Since $-2 = (-1)2$, by multiplicativity $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$, so $(\frac{-2}{p}) = 1$ precisely when $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both 1 or when $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both -1.

- Suppose $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both 1. That means $p \equiv 1 \bmod 4$ and $p \equiv 1, 7 \bmod 8$. Knowing a number mod 8 tells you what it has to be mod 4. Since $p \equiv 1 \bmod 8$ implies $p \equiv 1 \bmod 4$ and $p \equiv 7 \bmod 8$ implies $p \equiv 3 \bmod 4$, we have

$$p \equiv 1 \bmod 4 \text{ and } p \equiv 1, 7 \bmod 8 \iff p \equiv 1 \bmod 8.$$

[1] We write "□" to mean a number is a square.

Therefore $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both 1 precisely when $p \equiv 1 \bmod 8$.

- Suppose $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both -1, which means $p \equiv 3 \bmod 4$ and $p \equiv 3, 5 \bmod 8$. Arguing as in the previous case shows

$$p \equiv 3 \bmod 4 \text{ and } p \equiv 3, 5 \bmod 8 \Longleftrightarrow p \equiv 3 \bmod 8,$$

so $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both -1 precisely when $p \equiv 3 \bmod 8$.

The supplementary laws describing when $(\frac{-1}{p}) = 1$ and when $(\frac{2}{p}) = 1$ are worth memorizing. I've never been able to remember the rule describing when $(\frac{-2}{p}) = 1$, and when I need it I look it up.

Example 2.2. Let's use quadratic reciprocity to describe the primes $p \neq 2$ such that $(\frac{3}{p}) = 1$. Necessarily $p \neq 3$. By the main law of quadratic reciprocity,

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2\cdot(3-1)/2}\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

This is 1 when both factors are 1 or both are -1. We have

$$(-1)^{(p-1)/2} = 1 \Longleftrightarrow p \equiv 1 \bmod 4$$

and

$$\left(\frac{p}{3}\right) = 1 \Longleftrightarrow p \equiv 1 \bmod 3.$$

The conditions $p \equiv 1 \bmod 4$ and $p \equiv 1 \bmod 3$ together are equivalent to $p \equiv 1 \bmod 12$.

Also,

$$(-1)^{(p-1)/2} = -1 \Longleftrightarrow p \equiv 3 \bmod 4$$

and

$$\left(\frac{p}{3}\right) = -1 \Longleftrightarrow p \equiv 2 \bmod 3.$$

These two congruence conditions on p are the same as the single condition $p \equiv 11 \bmod 12$.

Thus, for $p \neq 2$, $(\frac{3}{p}) = 1$ if and only if $p \equiv 1, 11 \bmod 12$, or equivalently $p \equiv \pm 1 \bmod 12$.

Example 2.3. For which primes $p \neq 2$, when is $(\frac{-3}{p}) = 1$? Using the main law of quadratic reciprocity and the supplementary law for $(\frac{-1}{p})$,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Thus, for $p \neq 2$, $(\frac{-3}{p}) = 1$ if and only if $(\frac{p}{3}) = 1$, which means $p \equiv 1 \bmod 3$.

Example 2.4. For which primes $p \neq 2$ is $(\frac{5}{p}) = 1$? By quadratic reciprocity, $(\frac{5}{p}) = (\frac{p}{5})$, so $(\frac{5}{p}) = 1$ is the same as $(\frac{p}{5}) = 1$, which is equivalent to $p \equiv 1, 4 \bmod 5$. Thus when $p \neq 2$,

$$\left(\frac{5}{p}\right) = 1 \Longleftrightarrow p \equiv 1, 4 \bmod 5.$$

Example 2.5. For which primes $p \neq 2$ is $(\frac{-5}{p}) = 1$? We have

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{5}\right).$$

This is 1 when both terms are 1 or both are -1. Since

$$(-1)^{(p-1)/2} = 1 \Longleftrightarrow p \equiv 1 \bmod 4, \quad \left(\frac{p}{5}\right) = 1 \Longleftrightarrow p \equiv 1, 4 \bmod 5$$

and

$$(-1)^{(p-1)/2} = -1 \iff p \equiv 3 \bmod 4, \quad \left(\frac{p}{5}\right) = -1 \iff p \equiv 2, 3 \bmod 5,$$

we need to solve pairs of congruence conditions on p mod 4 and p mod 5:

$$\begin{aligned} p \equiv 1 \bmod 4, p \equiv 1 \bmod 5 &\iff p \equiv 1 \bmod 20, \\ p \equiv 1 \bmod 4, p \equiv 4 \bmod 5 &\iff p \equiv 9 \bmod 20, \\ p \equiv 3 \bmod 4, p \equiv 2 \bmod 5 &\iff p \equiv 7 \bmod 20, \\ p \equiv 3 \bmod 4, p \equiv 3 \bmod 5 &\iff p \equiv 3 \bmod 20 \end{aligned}$$

by the Chinese remainder theorem. Thus when $p \neq 2$, $(\frac{-5}{p}) = 1 \iff p \equiv 1, 3, 7, 9 \bmod 20$.

Example 2.6. For which primes $p \neq 2$ is $(\frac{10}{p}) = 1$?

Since $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p})$, we need either $(\frac{2}{p}) = 1$ and $(\frac{5}{p}) = 1$ or $(\frac{2}{p}) = -1$ and $(\frac{5}{p}) = -1$.

Suppose first that both $(\frac{2}{p})$ and $(\frac{5}{p})$ are 1. From the supplementary law, $(\frac{2}{p}) = 1$ if and only if $p \equiv 1, 7 \bmod 8$. From Example 2.4, $(\frac{5}{p}) = 1$ if and only if $p \equiv 1, 4 \bmod 5$. We need to solve

$$p \equiv 1 \text{ or } 7 \bmod 8 \quad \text{and} \quad p \equiv 1 \text{ or } 4 \bmod 5.$$

Each mod 8 condition and mod 5 condition is the same as one mod 40 condition. Altogether the four ways of pairing off the conditions mod 8 and mod 5 combine to give the congruences

$$p \equiv 1, 9, 31, 39 \bmod 40. \tag{2.1}$$

Now suppose that $(\frac{2}{p})$ and $(\frac{5}{p})$ equal -1. We have $(\frac{2}{p}) = -1$ if and only if $p \equiv 3, 5 \bmod 8$ and $(\frac{5}{p}) = -1$ if and only if $p \equiv 2, 3 \bmod 5$. Combine the congruences

$$p \equiv 3, 5 \bmod 8, \quad p \equiv 2, 3 \bmod 5$$

in pairs (one mod 8 and one mod 5) to give the congruences

$$p \equiv 3, 13, 27, 37 \bmod 40. \tag{2.2}$$

From (2.1) and (2.2), if $p \neq 2$, then $(\frac{10}{p}) = 1 \iff p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \bmod 40$.

Remark 2.7. It turns out when a is nonzero in $\mathbf{Z}$, the set of primes $\{p \neq 2 : (\frac{a}{p}) = 1\}$ can be described by congruence conditions on p mod $4|a|$. If $a = -1$ this means a condition on p mod 4 (see the rule for $(\frac{-1}{p})$), if $a = \pm 2$ this means conditions on p mod 8 (see the rule for $(\frac{2}{p})$ and Example 2.1), and if $a = 10$ this means a condition on p mod 40 (see Example 2.6). Sometimes we can use congruence conditions on p mod $|a|$ (see Examples 2.3 and 2.4 when a is -3 and 5), but those can also be written as conditions on p mod $4|a|$, *e.g.*, $p \equiv 1 \bmod 3$ is the same as $p \equiv 1, 7 \bmod 12$ when p is prime.

Exercises.

1. Use quadratic reciprocity to show $(\frac{6}{p}) = 1 \iff p \equiv 1, 5, 19, 23 \equiv \pm 1, \pm 5 \bmod 24$ and $(\frac{-6}{p}) = 1 \iff p \equiv 1, 5, 7, 11 \bmod 24$.

3. Elementary Cases of Dirichlet's Theorem

Dirichlet's theorem says that whenever a and m are relatively prime integers, there are infinitely many primes $p \equiv a \bmod m$. The general proof involves a combination of analysis and algebra. It turns out that some special cases of Dirichlet's theorem can be proved by much simpler methods that follow the strategy of Euclid's proof that there are infinitely many primes.

Theorem 3.1. *There are infinitely many primes $p \equiv 1 \bmod 4$ and there are infinitely many primes $p \equiv 3 \bmod 4$.*

Proof. It is easier to treat the case $p \equiv 3 \bmod 4$, so we do that first. If primes $p_1, \ldots, p_r$ satisfy $p_i \equiv 3 \bmod 4$ (such as 3, 7, and 11), consider

$$N = 4p_1 \cdots p_r - 1.$$

This number is odd, and by its definition $N \equiv 3 \bmod 4$.

Since $N > 1$, it has a prime factor. If every prime factor of N were $1 \bmod 4$ then we'd have $N \equiv 1 \bmod 4$ since N (as a *positive* integer) is the product of its prime factors (with repetition) and numbers that are $1 \bmod 4$ have a product that is also $1 \bmod 4$. But $N \equiv 3 \bmod 4$. Therefore N has a prime factor $p \not\equiv 1 \bmod 4$, which forces $p \equiv 3 \bmod 4$ since N is odd. The prime p is different from the p_i's since $p \mid N$ but no p_i divides N. Therefore no finite list of primes $\{p_1, \ldots, p_r\}$ that are $3 \bmod 4$ is all the primes that are $\equiv 3 \bmod 4$, so infinitely many primes are $3 \bmod 4$.

That reasoning does not work to show there are infinitely many primes $p \equiv 1 \bmod 4$ by changing the -1 to $+1$ in the definition of N because when an integer greater than 1 is $1 \bmod 4$ it need not have a prime factor that is $1 \bmod 4$: consider 21 and 33.

To show there are infinitely many primes $p \equiv 1 \bmod 4$, we will use *quadratic* expressions to define N (by comparison, the formula for N above is linear in the product $p_1 \cdots p_r$).

If $p_1, \ldots, p_r$ are all primes $\equiv 1 \bmod 4$ (such as 5, 13, and 17), let

$$N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.$$

Then N is odd and is $1 \bmod 4$. Since $N > 1$, it has a prime factor. Let p be a prime dividing N. Then

$$N \equiv 0 \bmod p \Longrightarrow -1 \equiv (2p_1 \cdots p_r)^2 \bmod p,$$

so $-1 \equiv \square \bmod p$, which implies $p \equiv 1 \bmod 4$. (We showed *each* prime factor of this N is $1 \bmod 4$.) The prime p is not any of $p_1, \ldots, p_r$ since those don't divide N. Thus no finite list of primes that are $\equiv 1 \bmod 4$ is complete, so infinitely many primes are $1 \bmod 4$.[2] □

Remark 3.2. The proof above for modulus 4 goes back to V. A. Lebesgue [3] in 1856.

Theorem 3.3. *There are infinitely many primes $p \equiv 4 \bmod 5$.*

Proof. One such prime is 19. If $p_1, \ldots, p_r$ are primes $\equiv 4 \bmod 5$, let

$$N = (2p_1p_2 \cdots p_r)^2 - 5 > 1.$$

Then N is not divisible by 2, 5, or any of $p_1, \ldots, p_r$. Let p be any prime factor of N, so $5 \equiv \square \bmod p$. Therefore, since $p \neq 2$ or 5, the characterization of when $5 \equiv \square \bmod p$

[2] Dirichlet's theorem has a quantitative aspect, saying when $(a, m) = 1$ that the set of primes $p \equiv a \bmod m$ has positive density among all primes. In the case $m = 4$ this says the sets of primes $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$ each have density $1/2$ in all the primes. The elementary proofs of special cases of Dirichlet's theorem that we are presenting here don't have any quantitative aspect like that.

(Example 2.4) tells us $p \equiv 1$ or $4 \bmod 5$: all prime factors of N are $1 \bmod 5$ or $4 \bmod 5$. To show N has a prime factor that is $4 \bmod 5$ we argue by contradiction. If every prime factor of N is $1 \bmod 5$, then $N \equiv 1 \bmod 5$, since N (as a *positive* integer) is the product of its prime factors (with repetition) and numbers that are $1 \bmod 5$ have a product that is also $1 \bmod 5$. However, $N \equiv 4 \bmod 5$ since $p_i^2 \equiv 1 \bmod 5$ for all i. (This is where we use all $p_i \equiv 4 \bmod 5$.) Therefore some prime factor p of N is not $1 \bmod 5$. The only option left is that $p \equiv 4 \bmod 5$. The prime p is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 4 \bmod 5$. □

In all these proofs, we used a polynomial whose values have special congruence conditions on their prime factors, *e.g.*, to show $p \equiv 4 \bmod 5$ infinitely often we relied on the fact that an integer of the form $n^2 - 5$ with n even and $n \not\equiv 0 \bmod 5$ is only divisible by primes $p \equiv 1, 4 \bmod 5$. (When $p \mid (n^2 - 5)$, $5 \bmod p$ is a square and $p \neq 2, 5$.) Table 1 is a summary of the polynomial and the square condition used for each progression above.

Progression	Polynomial	Square condition
1 mod 4	x^2+1	$-1 \equiv \square \bmod p$
3 mod 4	$x-1$	None
4 mod 5	x^2-5	$5 \equiv \square \bmod p$

TABLE 1. Polynomials used in elementary proofs of Dirichlet's theorem above.

Exercises.

1. Prove there are infinitely many primes $p \equiv 1 \bmod 3$ and infinitely many primes $p \equiv 2 \bmod 3$ in the style of the proof of Theorem 3.1. (Hint: To treat $p \equiv 1 \bmod 3$ use $N = (2p_1p_2 \cdots p_r)^2 + 3$.
2. Prove each of the following congruence conditions is satisfied by infinitely many primes using a Euclid-style proof.
   (i) $p \equiv 3 \bmod 8$ using $x^2 + 2$,
   (i) $p \equiv 5 \bmod 8$ using $x^2 + 1$,
   (ii) $p \equiv 7 \bmod 8$ using $x^2 - 2$,

4. Square patterns and Mordell's equation

The equation $y^2 = x^3 + k$, for $k \in \mathbf{Z}$, is called Mordell's equation, due to Mordell's work on it throughout his life. A natural number-theoretic task is describing all of its solutions in $\mathbf{Z}$ or $\mathbf{Q}$, either qualitatively (decide if there are finitely or infinitely many solutions in $\mathbf{Z}$ or $\mathbf{Q}$) or quantitatively (list or otherwise conveniently describe all such solutions). In 1920, Mordell [4] showed for each nonzero $k \in \mathbf{Z}$ that $y^2 = x^3 + k$ has finitely many integral solutions.[3] Siegel proved a similar finiteness theorem about the integral solutions to a wider class of cubic polynomial equations in two variables, so the finiteness of the number of integral solutions to a Mordell equation is also often attributed to Siegel too.

Example 4.1. The only integral solutions to $y^2 = x^3 - 2$ are $(x, y) = (3, \pm 5)$. This example goes back to Fermat, who challenged British mathematicians to prove it.

[3] Large tables of k and the integral solutions of $y^2 = x^3 + k$ are at https://hr.userweb.mwn.de/numb/mordell.html and https://secure.math.ubc.ca/∼bennett/BeGa-data.html.

We will use square patterns mod primes to show certain Mordell equations have *no* integral solutions. Specifically, we will use the following descriptions of when -1, 2, and -2 are squares modulo odd primes p:

$$\begin{aligned} -1 \equiv \Box \bmod p &\iff p \equiv 1 \bmod 4, \\ 2 \equiv \Box \bmod p &\iff p \equiv 1, 7 \bmod 8, \\ -2 \equiv \Box \bmod p &\iff p \equiv 1, 3 \bmod 8. \end{aligned}$$

Theorem 4.2. *The equation $y^2 = x^3 + 11$ has no integral solutions.*

Proof. Assume there is an integral solution (x, y) and reduce modulo 4:

$$y^2 \equiv x^3 + 3 \bmod 4.$$

Here is a table of values of y^2 and $x^3 + 3$ modulo 4:

y	$y^2 \bmod 4$	x	$x^3 + 3 \bmod 4$
0	0	0	3
1	1	1	0
2	0	2	3
3	1	3	2

The only common value of $y^2 \bmod 4$ and $x^3 + 3 \bmod 4$ is 0, so y is even and $x \equiv 1 \bmod 4$.

Now rewrite $y^2 = x^3 + 11$ by adding 16 to both sides:

$$y^2 + 16 = x^3 + 27 = (x + 3)(x^2 - 3x + 9). \tag{4.1}$$

The integer $x^2 - 3x + 9$ is positive since it equals $(x - 3/2)^2 + 27/4$, which is a sum of positive numbers. Since $x \equiv 1 \bmod 4$, we get $x^2 - 3x + 9 \equiv 3 \bmod 4$, so $x^2 - 3x + 9$ is a positive integer that is 3 mod 4. Therefore, by the same reasoning used in the earlier proof that there are infinitely many primes congruent to 3 mod 4, $x^2 - 3x + 9$ must have a prime factor p with $p \equiv 3 \bmod 4$. Then $y^2 + 16 \equiv 0 \bmod p$ by (4.1), so $-16 \equiv \Box \bmod p$. Since p is odd, we can turn that congruence into $-1 \equiv \Box \bmod p$, which implies $p \equiv 1 \bmod 4$ since p is odd, and this contradicts $p \equiv 3 \bmod 4$. □

Remark 4.3. The equation $y^2 = x^3 + 11$ has rational solutions, such as $(x, y) = (-7/4, 19/8)$. In fact it has infinitely many rational solutions.

Remark 4.4. A common elementary way to show a polynomial equation with integer coefficients has no **Z**-solution is to show it has no solution mod m for some $m \geq 2$, *e.g.*, $x^2 - 10y^2 = 2$ has no **Z**-solution since it has no solution mod 5. That method can't be used to prove some $y^2 = x^3 + k$ has no **Z**-solution since the congruence $y^2 \equiv x^3 + k \bmod m$ has a solution for all $m \geq 2$ no matter what k is. Some discussion about this when m is prime and a prime power can be read at https://math.stackexchange.com/questions/875983/ and https://mathoverflow.net/questions/134352.

Theorem 4.5. *The equation $y^2 = x^3 - 6$ has no integral solutions.*

Proof. Assume there is an integral solution. If x is even then $y^2 \equiv -6 \equiv 2 \bmod 8$, but $2 \bmod 8$ is not a square. Therefore x is odd, so y is odd and $x^3 = y^2 + 6 \equiv 7 \bmod 8$. Also $x^3 \equiv x \bmod 8$ (true for all odd x), so $x \equiv 7 \bmod 8$.

Rewrite $y^2 = x^3 - 6$ as

$$y^2 - 2 = x^3 - 8 = (x - 2)(x^2 + 2x + 4), \tag{4.2}$$

with $x^2+2x+4 \equiv 7^2+2\cdot 7+4 \equiv 3 \bmod 8$. Since $x^2+2x+4=(x+1)^2+3$ is positive, it must have a prime factor $p \equiv \pm 3 \bmod 8$ because if all of its prime factors are $\pm 1 \bmod 8$ then $x^2+2x+4 \equiv \pm 1 \bmod 8$, which is not true. Let p be a prime factor of x^2+2x+4 with $p \equiv \pm 3 \bmod 8$. Since p divides y^2-2 by (4.2), we get $y^2 \equiv 2 \bmod p$. Thus $2 \equiv \Box \bmod p$, so $p \equiv \pm 1 \bmod 8$, which is a contradiction.

We can get a contradiction using the factor $x-2$ also. Since $x \equiv 7 \bmod 8$, $x-2 \equiv 5 \bmod 8$. Also $x-2>0$, since if $x \leq 2$ and $x-2 \equiv 5 \bmod 8$ then $x \leq -1$, but then x^3-6 is negative so it can't be a square. From $x-2$ being positive and congruent to 5 mod 8, it has a prime factor $p \equiv \pm 3 \bmod 8$ and then $y^2 \equiv 2 \bmod p$ and we get a contradiction in the same way as before. □

Theorem 4.6. *The equation $y^2=x^3+6$ has no integral solutions.*

Proof. Mordell [5, p. 22-23], [6, p. 70] proved this using $\mathbf{Z}[\sqrt{6}]$. I learned the simpler method we use here, which resembles the proof of Theorem 4.5, from Shiv Gupta and Tracy Driehaus.

Assume there is an integral solution (x,y) to $y^2=x^3+6$. First we will show x is odd, and in fact $x \equiv 3 \bmod 8$. If x is even then $y^2 \equiv 6 \bmod 8$, which is impossible. Thus x is odd, so y is odd and $x^3=y^2-6 \equiv -5 \equiv 3 \bmod 8$. Since $x^3 \equiv x \bmod 8$, we have $x \equiv 3 \bmod 8$.

Rewrite $y^2=x^3+6$ as

$$y^2+2=x^3+8=(x+2)(x^2-2x+4), \tag{4.3}$$

with $x^2-2x+4 \equiv 3^2-2\cdot 3+4 \equiv 7 \bmod 8$. For each prime factor p of x^2-2x+4, $y^2+2 \equiv 0 \bmod p$, so $-2 \equiv \Box \bmod p$, and therefore $p \equiv 1, 3 \bmod 8$ (Example 2.1). Then, since $x^2-2x+4=(x-1)^2+3$ is positive and $3^2 \equiv 1 \bmod 8$, x^2-2x+4 is 1 or 3 mod 8. We showed before that this number is 7 mod 8, so we have a contradiction.

To get a contradiction using the factor $x+2$, first note that this number is positive, since if $x+2<0$ then $y^2+2 \leq 0$, which is impossible. For a prime p dividing $x+2$, $y^2+2 \equiv 0 \bmod p$, so $p \equiv 1$ or $3 \bmod 8$. Therefore $x+2 \equiv 1$ or $3 \bmod 8$. However, since $x \equiv 3 \bmod 8$ we have $x+2 \equiv 5 \bmod 8$, which is a contradiction. □

Our next theorem uses both conditions for $-1 \bmod p$ and $-2 \bmod p$ to be squares.

Theorem 4.7. *The equation $y^2=x^3-24$ has no integral solutions.*

Proof. We take our argument from [**?**, pp. 271–272], which is based on [**?**, p. 201].

Assuming there is an integral solution (x,y), we show x is even. Rewrite $y^2=x^3-24$ as

$$y^2+16=x^3-8=(x-2)(x^2+2x+4).$$

The factor x^2+2x+4 equals $(x+1)^2+3$, which is at least 3. If x is odd then $(x+1)^2+3 \equiv 3 \bmod 4$, so $(x+1)^2+3$ has a prime factor p such that $p \equiv 3 \bmod 4$. Then $y^2 \equiv -16 \bmod p$, so $-1 \equiv \Box \bmod p$. This contradicts the condition $p \equiv 3 \bmod 4$. Thus x is even, so y is even.

From $y^2=x^3-24$ we get $8 \mid y^2$, so $4 \mid y$. Write $x=2x'$ and $y=4y'$. Then $16y'^2=8x'^3-24$, which implies $2y'^2=x'^3-3$, so x' is odd and $x'>1$. Rewrite $2y'^2=x'^3-3$ as

$$2(y'^2+2)=x'^3+1=(x'+1)(x'^2-x'+1).$$

The factor $x'^2-x'+1$ is odd and greater than 1. Let p be a prime factor of it, so $y'^2 \equiv -2 \bmod p$, which implies $p \equiv 1$ or $3 \bmod 8$. Then $x'^2-x'+1$ is a product of primes that are all 1 or 3 mod 8, so $x'^2-x'+1 \equiv 1$ or $3 \bmod 8$. We have

$$y'^2 \equiv 0, 1, \text{or } 4 \bmod 8 \Longrightarrow x'^3=2y'^2+3 \equiv 3 \text{ or } 5 \bmod 8 \Longrightarrow x' \equiv 3 \text{ or } 5 \bmod 8.$$

Then $x'^2 - x' + 1 \equiv 1 - x' + 1 \equiv 2 - x' \equiv 5$ or $7 \bmod 8$. That contradicts $x'^2 - x' + 1 \equiv 1$ or $3 \bmod 8$. □

The equations $y^2 = x^3 + 6$, $y^2 = x^3 - 6$, and $y^2 = x^3 - 24$ each have no rational solution, but proving that is much more involved than the arguments above proving that they have no integral solution.

In the exercises below, use methods like those used above. In each case, begin by showing x is odd (this is trickier for the third exercise).

Exercises.

1. Show $y^2 = x^3 - 3$ has no integral solution. (Hint: $y^2 + 4 = x^3 + 1$).
2. Show $y^2 = x^3 - 9$ has no integral solution. (Hint: $y^2 + 1 = x^3 - 8$).
3. Show $y^2 = x^3 - 12$ has no integral solution. (Hint: $y^2 + 4 = x^3 - 8$).

5. Solvability of $p = x^2 - dy^2$

When d in $\mathbf{Z}$ is not a square, determining prime values of $x^2 - dy^2$ is a task in number theory going back to the beginning of the subject. Fermat and Euler both looked at the cases $d = -1$ and $d = 2$: $x^2 + y^2$ and $x^2 - 2y^2$. They proved for odd primes p that

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4$$

and

$$p = x^2 - 2y^2 \iff p \equiv \pm 1 \bmod 8.$$

The congruence conditions on the right sides are the odd primes such that $-1 \equiv \Box \bmod p$ and $2 \equiv \Box \bmod p$. There is in fact a general connection between determining when a prime p has the form $x^2 - dy^2$ in $\mathbf{Z}$ and when $d \equiv \Box \bmod p$. We'll prove the simpler direction first.

Theorem 5.1. *Let p be prime and d in $\mathbf{Z}$ not be a square. If $p = x^2 - dy^2$ in $\mathbf{Z}$ then $d \equiv \Box \bmod p$.*

Proof. When $p = x^2 - dy^2$ in $\mathbf{Z}$, $p \nmid y$ by contradiction: if $p \mid y$ then $p \mid x^2$, so $p \mid x$, but then $x^2 - dy^2$ is divisible by p^2, which contradicts $x^2 - dy^2$ being equal to p.

Now reduce the equation $p = x^2 - dy^2$ modulo p: $x^2 \equiv dy^2 \bmod p$. Since $y \not\equiv 0 \bmod p$, divide by y^2 to get $d \equiv \Box \bmod p$. □

The converse to Theorem 5.1 is true when $d = -1$ and when $d = 2$. That is,

$$-1 \equiv \Box \bmod p \Longrightarrow p = x^2 + y^2 \text{ for some } x, y \in \mathbf{Z},$$
$$2 \equiv \Box \bmod p \Longrightarrow p = x^2 - 2y^2 \text{ for some } x, y \in \mathbf{Z}.$$

However, in general the converse implication

$$d \equiv \Box \bmod p \Longrightarrow p = x^2 - dy^2 \text{ for some } x, y \in \mathbf{Z} \tag{5.1}$$

has counterexamples. Here are two cases where (5.1) fails.

Example 5.2. Taking $d = 10$ and $p = 3$, we have $10 \equiv 1 \equiv \Box \bmod 3$, but $3 \neq x^2 - 10y^2$ in $\mathbf{Z}$ by reducing mod 5, since $3 \not\equiv \Box \bmod 5$.

Example 5.3. Taking $d = 3$ and $p = 11$, we have $3 \equiv 5^2 \equiv \Box \bmod 11$, but $11 \neq x^2 - 3y^2$ in $\mathbf{Z}$ by reducing mod 3 since $11 \equiv 2 \not\equiv \Box \bmod 3$.

There is a result very close to (5.1) when the ring $\mathbf{Z}[\sqrt{d}] = \{a+b\sqrt{d} : a, b \in \mathbf{Z}\}$ has unique factorization. When d is small, $\mathbf{Z}[\sqrt{d}]$ has unique factorization when $d = -1$ (that's the Gaussian integers $\mathbf{Z}[i]$), $d = \pm 2$, and $d = 3$ because these rings are all Euclidean domains. There is not unique factorization in $\mathbf{Z}[\sqrt{d}]$ when $d = -3$ and $d = \pm 5$. Techniques from algebraic number theory allow you to prove a ring like $\mathbf{Z}[\sqrt{d}]$ has unique factorization without having to determine whether or not it is Euclidean. As an example, $\mathbf{Z}[\sqrt{14}]$ was known in the 19th century to have unique factorization, but it was proved to be Euclidean (by Malcolm Harper) only in 2004. Rings with unique factorization need not be Euclidean: see Section 5 in https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf.

Theorem 5.4. *Let d be an integer that is not a square. If $\mathbf{Z}[\sqrt{d}]$ has unique factorization then for all primes p,*

$$d \equiv \Box \bmod p \Longrightarrow \pm p = x^2 - dy^2 \bmod p \text{ for some } x, y \in \mathbf{Z}.$$

The implication here differs from (5.1) in a slight way: it says p *or* $-p$ is $x^2 - dy^2$ in $\mathbf{Z}$. Maybe $-p$ has that form while p does not. Consider $d = 3$: since $\mathbf{Z}[\sqrt{3}]$ has unique factorization, Theorem 5.4 says that if $3 \equiv \Box \bmod p$ then p or $-p$ is $x^2 - 3y^2$. So from $3 \equiv 5^2 \bmod 11$, either 11 or -11 is $x^2 - 3y^2$ in $\mathbf{Z}$. We saw $11 \neq x^2 - 3y^2$ in $\mathbf{Z}$ in Example 5.3, but -11 is $x^2 - 3y^2$ using $x = 1$ and $y = 2$. Thus the minus sign in $\pm p$ in Theorem 5.4 is essential in general. Now let's prove Theorem 5.4.

Proof. By hypothesis $d \equiv n^2 \bmod p$ for some integer n , so $p \mid (n^2 - d)$ in $\mathbf{Z}$. Inside $\mathbf{Z}[\sqrt{d}]$ we have $n^2 - d = (n + \sqrt{d})(n - \sqrt{d})$, so $p \mid (n + \sqrt{d})(n - \sqrt{d})$ in $\mathbf{Z}[\sqrt{d}]$. We will use this divisibility relation to show p is reducible in $\mathbf{Z}[\sqrt{d}]$.[4]

The number p is not a unit in $\mathbf{Z}[\sqrt{d}]$: we can't have $p(a + b\sqrt{d}) = 1$ for a and b in $\mathbf{Z}$. Thus p is either reducible or irreducible in $\mathbf{Z}[\sqrt{d}]$. Because $\mathbf{Z}[\sqrt{d}]$ has unique factorization, if p were irreducible then

$$p \mid (n + \sqrt{d})(n - \sqrt{d}) \Longrightarrow p \mid (n + \sqrt{d}) \text{ or } p \mid (n - \sqrt{d}) \text{ in } \mathbf{Z}[\sqrt{d}].$$

Thus $p(a + b\sqrt{d}) = n \pm \sqrt{d}$ for some choice of sign on the right side and some a and b in $\mathbf{Z}$. Then $pb = \pm 1$ in $\mathbf{Z}$, which is a contradiction. We have shown p is not reducible in $\mathbf{Z}[\sqrt{d}]$, so it must be reducible:

$$p = \alpha\beta \tag{5.2}$$

where α and β in $\mathbf{Z}[\sqrt{d}]$ are *not* units.

To make more progress we will use the norm map on $\mathbf{Z}[\sqrt{d}]$. When $\alpha = x + y\sqrt{d}$ with x and y in $\mathbf{Z}$, set $\overline{\alpha} = x - y\sqrt{d}$ and the norm of α is defined to be

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = x^2 - dy^2.$$

This is in $\mathbf{Z}$ and a direct calculation shows the norm is multiplicative: $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ for all α and β in $\mathbf{Z}[\sqrt{d}]$. Also $\mathrm{N}(m) = m^2$ when $m \in \mathbf{Z}$. Note $x^2 - dy^2 \geq 0$ when $d < 0$ ($\mathrm{N}(x+yi) = x^2+y^2$ and $\mathrm{N}(x+y\sqrt{-2}) = x^2+2y^2$), while x^2-dy^2 may be positive or negative when $d > 0$ depending on x and y, *e.g.*, $\mathrm{N}(1+2\sqrt{2}) = 1-8 = -7$ and $\mathrm{N}(3+\sqrt{2}) = 9-2 = 7$.

Returning to (5.2), take the norm of both sides:

$$p^2 = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta) \text{ in } \mathbf{Z}. \tag{5.3}$$

[4] Prime numbers often become reducible in quadratic rings: in $\mathbf{Z}[i]$, 3 is irreducible but 2 and 5 are not: $2 = (1 + i)(1 - i)$ and $5 = (1 + 2i)(1 - 2i)$.

The possible values of $\mathrm{N}(\alpha)$ are ± 1, $\pm p$, or $\pm p^2$ (norms may be negative when $d > 0$).

If $\mathrm{N}(\alpha) = 1$ then $\alpha\overline{\alpha} = 1$, so α is a unit, which is false. If $\mathrm{N}(\alpha) = -1$ then $\alpha\overline{\alpha} = -1$, so $\alpha(-\overline{\alpha}) = 1$ and again α is a unit, which is again false. Thus $\mathrm{N}(\alpha) \neq \pm 1$. Similarly, $\mathrm{N}(\beta) \neq \pm 1$, which means $\mathrm{N}(\alpha) \neq \pm p^2$. The only options remaining for $\mathrm{N}(\alpha)$ are $\pm p$. Writing $\alpha = x + y\sqrt{d}$, we get

$$x^2 - dy^2 = \pm p. \qquad \square$$

When $d < 0$, we never have $-p = x^2 - dy^2$ in $\mathbf{Z}$ since $-d > 0$, so for negative d the conclusion in Corollary 5.5 can be written as: $p = x^2 - dy^2$ in $\mathbf{Z}$ if and only if $d \equiv \square \bmod p$. When $d > 0$, we can turn $-p = x^2 - dy^2$ into $p = x^2 - dy^2$ (for new x and y, of course) if we can write -1 as a norm from $\mathbf{Z}[\sqrt{d}]$. Indeed, when $-p = x^2 - dy^2 = \mathrm{N}(x + y\sqrt{d})$ and $-1 = a^2 - db^2 = \mathrm{N}(a + b\sqrt{d})$, multiply the equations to get

$$p = \mathrm{N}((a + b\sqrt{d})(x + y\sqrt{d})) = x'^2 - dy'^2$$

where we set $x' + y'\sqrt{d} = (a + b\sqrt{d})(x + y\sqrt{d})$. For example, from $-7 = 1^2 - 2 \cdot 2^2 = \mathrm{N}(1 + 2\sqrt{2})$ and $-1 = \mathrm{N}(1 + \sqrt{2})$, we get $7 = \mathrm{N}((1 + 2\sqrt{2})(1 + \sqrt{2}) = \mathrm{N}(5 + 3\sqrt{2}) = 5^2 - 2 \cdot 7^2$. Also $-1 = \mathrm{N}(1 - \sqrt{2})$, so $7 = \mathrm{N}((1 + 2\sqrt{2})(1 - \sqrt{2})) = \mathrm{N}(-3 + \sqrt{2}) = (-3)^2 - 2 \cdot 1^2 = 3^2 - 2 \cdot 1^2$.

Corollary 5.5. *Let $d \in \mathbf{Z}$ not be a square. When $\mathbf{Z}[\sqrt{d}]$ has unique factorization and p is prime, p or $-p$ is $x^2 - dy^2$ in $\mathbf{Z}$ if and only if $d \equiv \square \bmod p$.*

If either $d < 0$, or if $d > 0$ and $-1 = a^2 - db^2$ in $\mathbf{Z}$, then $p = x^2 - dy^2$ in $\mathbf{Z}$ if and only if $d \equiv \square \bmod p$.

Proof. The direction ($\Rightarrow$) is due to Theorem 5.1 (while that proof only looked at $p = x^2 - dy^2$, the same reasoning works for $-p = x^2 - dy^2$) and does not require any hypotheses about $\mathbf{Z}[\sqrt{d}]$. The direction ($\Leftarrow$) is Theorem 5.4.

That we can drop the condition about $-p$ when $d < 0$ or -1 is a norm from $\mathbf{Z}[\sqrt{d}]$ when $d > 0$ is explain by the paragraph preceding this corollary. $\square$

Example 5.6. The rings $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{-2}]$, and $\mathbf{Z}[\sqrt{3}]$ all have unique factorization since they are Euclidean domains and $-1 = \mathrm{N}(1 + \sqrt{2})$. Taking $d = -1$, 2, -2, and 3 in Corollary 5.5,

$$p = x^2 + y^2 \text{ in } \mathbf{Z} \iff -1 \equiv \square \bmod p,$$
$$p = x^2 - 2y^2 \text{ in } \mathbf{Z} \iff 2 \equiv \square \bmod p,$$
$$p = x^2 + 2y^2 \text{ in } \mathbf{Z} \iff -2 \equiv \square \bmod p,$$
$$\pm p = x^2 - 3y^2 \text{ in } \mathbf{Z} \iff 3 \equiv \square \bmod p.$$

Example 5.7. Being able to write a prime p as $x^2 + 5y^2$ in $\mathbf{Z}$ requires $-5 \equiv \square \bmod p$ by Theorem 5.1, but we don't expect the converse to hold since $\mathbf{Z}[\sqrt{-5}]$ does not have unique factorization. Indeed, the converse direction really doesn't hold: see Exercise 5.2.

Remark 5.8. When d is squarefree, $d \not\equiv 1 \bmod 4$, and $\mathbf{Z}[\sqrt{d}]$ does not have unique factorization, the converse to Theorem 5.1 always fails: there are infinitely many primes p such that $d \equiv \square \bmod p$ but p and $-p$ are not $x^2 - dy^2$ in $\mathbf{Z}$. See Exercise 5.4.

Exercises.

1. The first 5 primes p such that $-2 \equiv \square \bmod p$ are 2, 3, 11, 17, 19. Theorem 5.6 says these primes are all $x^2 + 2y^2$ in $\mathbf{Z}$. Determine such x and y for each of these primes.

2. By Example 2.4, $5 \equiv \Box \bmod p$ if and only if $p = 2$ or $p \equiv 1, 4 \bmod 5$.

   a) Show that if a prime p satisfies $-p = x^2 - 5y^2$ for some x and y in $\mathbf{Z}$, then also $p = x'^2 - 5y'^2$ for some x' and y' in $\mathbf{Z}$.

   b) Find a prime p such that $5 \equiv \Box \bmod p$ but p doesn't have the form $x^2 - 5y^2$ in $\mathbf{Z}$. By Corollary 5.5, we can conclude that $\mathbf{Z}[\sqrt{5}]$ does not have unique factorization without writing down a specific counterexample to unique factorization in $\mathbf{Z}[\sqrt{5}]$.

   c) Verify that the equation $4 = 2 \cdot 2 = (\sqrt{5}+1)(\sqrt{5}-1)$ is an explicit counterexample to unique factorization in $\mathbf{Z}[\sqrt{5}]$.

3. By Example 2.5, $(\frac{-5}{p}) = 1 \iff p \equiv 1, 3, 7, 9 \bmod 20$. Since $\mathbf{Z}[\sqrt{-5}]$ does not have unique factorization, we don't expect for primes p that $-5 \equiv \Box \bmod p$ is always equivalent to $p = x^2 + 5y^2$ in $\mathbf{Z}$.

   a) Show that when $p \equiv 3, 7 \bmod 20$, $p \neq x^2 + 5y^2$ in $\mathbf{Z}$.

   b) The primes below 100 that are $1, 9 \bmod 20$ are 29, 41, 61, and 89. In each case, show $p = x^2 + 5y^2$ in $\mathbf{Z}$.

4. This exercise is for those who have studied algebraic number theory. Suppose $\mathbf{Z}[\sqrt{d}]$ is the ring of integers of $\mathbf{Q}(\sqrt{d})$, so d is squarefree and $d \not\equiv 1 \bmod 4$.

   a) If $\mathfrak{p}$ is a prime ideal in $\mathbf{Z}[\sqrt{d}]$ whose ideal norm is the prime number p, then show $\pm p = x^2 - dy^2$ in $\mathbf{Z}$ if and only if $\mathfrak{p}$ is a principal ideal.

   b) When a prime p splits completely in $\mathbf{Z}[\sqrt{-5}]$, so $(p) = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct prime ideals, show $\mathfrak{p}$ and $\mathfrak{p}$' are principal if and only if $p \equiv 1, 9 \bmod 20$. (Hint: the class number of $\mathbf{Q}(\sqrt{-5})$ is 2 and the nontrivial ideal class is represented by the ideal $\mathfrak{p}_2$ lying over 2, where $(2) = \mathfrak{p}_2^2$. When $\mathfrak{p}$ is nonprincipal, $\mathfrak{p}\mathfrak{p}_2$ is principal, say $(x + y\sqrt{-5})$, so taking ideal norms shows $2p = x^2 + 5y^2$.)

   c) When $\mathbf{Z}[\sqrt{d}]$ does not have unique factorization, so the class number h of $\mathbf{Q}(\sqrt{d})$ is greater than 1, show the set of principal prime ideals in $\mathbf{Z}[\sqrt{d}]$ has density $1/h$ in the set of all prime ideals in $\mathbf{Z}[\sqrt{d}]$, so the set of non-principal prime ideals in $\mathbf{Z}[\sqrt{d}]$ has density $1 - 1/h$. Explain why this implies there are infinitely many non-principal prime ideals in $\mathbf{Z}[\sqrt{d}]$ with prime ideal norm and thus infinitely many prime numbers p such that $d \equiv \Box \bmod p$ and neither p nor $-p$ is $x^2 - dy^2$ in $\mathbf{Z}$.

6. Solving $x^2 \equiv a \bmod p$ when a solution exists

For an odd prime p and an integer $a \not\equiv 0 \bmod p$, suppose we use quadratic reciprocity to see that $(\frac{a}{p}) = 1$, so the congruence $x^2 \equiv a \bmod p$ has a solution Is there a systematic way to actually find a solution (not just by a brute force search)? We will describe two such methods: the Tonelli–Shanks algorithm and Cipolla's algorithm. They both need as input a quadratic non-residue mod p.

The Tonelli–Shanks algorithm was first discovered by Alberto Tonelli[5] [8] and rediscovered many years later by Dan Shanks [7]. To motivate it, let's suppose $(\frac{a}{p}) = 1$ and $p \equiv 3 \bmod 4$. A direct formula for a square root of $a \bmod p$ in this case is $a^{(p+1)/4}$:

$$(a^{(p+1)/4})^2 = a^{(p+1)/2} = a^{(p-1)/2}a \equiv a \bmod p$$

since $a^{(p-1)/2} \equiv 1 \bmod p$. The number $a^{(p+1)/4} \bmod p$ does not work when $p \equiv 1 \bmod 4$ since $(p+1)/4 \notin \mathbf{Z}$. And using $(p-1)/4$ instead of $(p+1)/4$ in the exponent when $p \equiv 1 \bmod 4$ also does not lead to a square root of $a \bmod p$ since $(a^{(p-1)/4})^2 = a^{(p-1)/2} \equiv 1 \bmod p$.

[5] He is not the analyst Tonelli in the Fubini–Tonelli theorem.

What can we use as a substitute for $(p+1)/4$ when $p \equiv 1 \bmod 4$? Write

$$p - 1 = 2^e k$$

where $e \geq 1$ and k is odd, so 2^e is the highest power of 2 dividing $p-1$. If $p \equiv 3 \bmod 4$ then $e = 1$ and $(p+1)/4 = (2k+2)/4 = (k+1)/2$. Even if $p \equiv 1 \bmod 4$, $(k+1)/2$ is still an integer, so we will use $(k+1)/2$ for all p as a replacement for $(p+1)/4$ from the case $p \equiv 3 \bmod 4$.

Set

$$x_1 = a^{(k+1)/2} \bmod p.$$

Then

$$x_1^2 = a^{k+1} = aa^k = ay_1 \bmod p. \tag{6.1}$$

where $y_1 \equiv a^k \bmod p$.

The order of $y_1 \bmod p$ divides 2^{e-1} since

$$y_1^{2^{e-1}} = (a^k)^{2^{e-1}} = a^{2^{e-1}k} = a^{(p-1)/2} \equiv 1 \bmod p,$$

where the last step is due to $a \equiv \square \bmod p$. If $y_1 \equiv 1 \bmod p$ then $x_1^2 \equiv a \bmod p$ and we are done. What if $y_1 \not\equiv 1 \bmod p$, meaning its order is a factor of 2^{e-1} other than 1?

The idea now is to extend (6.1) to a sequence of congruences

$$x_2^2 \equiv y_2 a \bmod p, \ x_3^2 \equiv y_3 a \bmod p, \ \ldots, \ x_i^2 \equiv y_i a \bmod p, \ \ldots \tag{6.2}$$

where $y_i \bmod p$ has order dividing 2^{e-i}, so these orders are dropping. In e steps we'll reach $x_e^2 \equiv y_e a \bmod p$ where $y_e \bmod p$ has order dividing $2^{e-e} = 1$, so $y_e \equiv 1 \bmod p$ and thus $x_e^2 \equiv a \bmod p$. In practice we may get $y_i \equiv 1 \bmod p$ for some $i < e$, so $x_i^2 \equiv a \bmod p$ and we are then done in fewer than e steps.

To build the congruences (6.2) we will use powers of a number mod p with order exactly 2^e, and this is where a quadratic non-residue comes in. Use quadratic reciprocity to find b such that $b \not\equiv \square \bmod p$, so $b^{(p-1)/2} \equiv -1 \bmod p$. Such b may be found by letting $b = 2, 3, \ldots$ and computing $(\frac{b}{p})$ until $(\frac{b}{p}) = -1$. In practice it does not take long to find such b, even by random guessing since half the nonzero numbers mod p are quadratic non-residues. The generalized Riemann hypothesis implies there is such $b \leq 2(\log p)^2$.

From $b^{(p-1)/2} \equiv -1 \bmod p$, set $c := b^k \bmod p$. This number $c \bmod p$ has order 2^e since

$$c^{2^e} = (b^k)^{2^e} = b^{2^e k} = b^{p-1} \equiv 1 \bmod p, \quad c^{2^{e-1}} = (b^k)^{2^{e-1}} = b^{2^{e-1}k} = b^{(p-1)/2} \equiv -1 \bmod p,$$

so $c \bmod p$ has order dividing 2^e and not dividing 2^{e-1}. Thus its order is exactly 2^e. When $0 \leq i \leq e$, $c^{2^{e-i}}$ has order $2^e/2^{e-i} = 2^i$, so we get numbers with order $1, 2, 2^2, 2^3, \ldots, 2^e$ by using $c^{2^e}, c^{2^{e-1}}$, $c^{2^{e-2}}$, $c^{2^{e-3}}$, and so on up to $c^{2^{e-e}} = b^k$ with order 2^e.

Returning to (6.1), where we assume $y_1 \not\equiv 1 \bmod p$, its order is 2^j where $1 \leq j \leq e-1$. Also $c^{2^{e-j}}$ has order 2^j. It turns out that the product $y_1 c^{2^{e-j}}$ has 2-power order less than 2^j by the following fact.

Fact: in $(\mathbf{Z}/(p))^\times$, if two elements have equal 2-power order greater than 1, then their product has smaller 2-power order.

This is due to $(\mathbf{Z}/(p))^\times$ being cyclic, so two elements with equal 2-power order generate the same subgroup, and in a nontrivial cyclic 2-group with order, say, 2^r the product of two elements with order 2^r has order dividing 2^{r-1} (see Exercise 6.1).

Multiply both sides of (6.1) by $c^{2^{e-j}}$, which is a square since $e-j \geq 1$:

$$x_1^2 c^{2^{e-j}} \equiv a y_1 c^{2^{e-j}} \bmod p \Longrightarrow (x_1 c^{2^{e-1-j}})^2 \equiv a(y_1 c^{2^{e-j}}) \bmod p.$$

Set $x_2 = x_1 c^{2^{e-1-j}} \bmod p$ and $y_2 = y_1 c^{2^{e-j}} \bmod p$, so

$$x_2^2 \equiv a y_2 \bmod p \tag{6.3}$$

where y_2 has 2-power order $2^{j'}$ and $j' \leq j-1 \leq e-2$. If $j'=0$ then $y_2 \equiv 1 \bmod p$ and $x_2^2 \equiv a \bmod p$, so we're done.

If $j' \neq 0$, so $1 \leq j' \leq e-2$, then $c^{2^{e-j'}} \bmod p$ has order $2^{j'}$, so by the Fact above $y_2 c^{2^{e-j'}} \bmod p$ has 2-power order less than $2^{j'}$. Multiply both sides of (6.3) by $c^{2^{e-j'}}$ to get

$$(x_2 c^{2^{e-1-j'}})^2 \equiv a(y_2 c^{2^{e-j'}}) \bmod p.$$

Set $x_3 = x_2 c^{2^{e-1-j'}} \bmod p$ and $y_3 = y_2 c^{2^{e-j'}} \bmod p$, so

$$x_3^2 \equiv a y_3 \bmod p \tag{6.4}$$

where y_3 has 2-power order $2^{j''}$ and $j'' \leq j'-1 \leq e-3$. If $j''=0$ then $y_3 \equiv 1 \bmod p$ and $x_3^2 \equiv a \bmod p$, so we're done. Otherwise we can continue producing the congruences as in (6.2) where the term $y_i \bmod p$ has 2-power order dividing 2^{e-i}, so we'll eventually have some $y_i \equiv 1 \bmod p$ (with $i \leq e$) and then $x_i^2 \equiv a \bmod p$.

Example 6.1. The number $p = 1249$ is prime. Since $p \equiv 1 \bmod 8$, by quadratic reciprocity $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p}) = (\frac{p}{5}) = (\frac{4}{5}) = 1$. To use the Tonelli–Shanks algorithm to solve $x^2 \equiv 10 \bmod p$ we need a quadratic non-residue mod p. Check $(\frac{19}{p}) = -1$, so we can use $b = 19$.

We have $p-1 = 2^5 \cdot 39 = 2^e k$. Set $c = b^k = 19^{39} \equiv 305 \bmod p$, which has order 32. (The proof of the Tonelli–Shanks algorithm said $c \bmod p$ has order exactly 2^e.)

Set $a = 10$ and $x_1 = a^{(k+1)/2} \equiv 294 \bmod p$. Then $x_1^2 \equiv 10y_1 \bmod p$ where $y_1 = 10^k \equiv 650 \bmod p$, and $y_1 \bmod p$ has order 16. Also $c^2 \bmod p$ has order 16. Then

$$x_1^2 c^2 \equiv 10 y_1 c^2 \bmod p \Longrightarrow (x_1 c)^2 \equiv 10(y_1 c^2) \bmod p.$$

Set $x_2 = x_1 c \equiv 991 \bmod p$ and $y_2 = y_1 c^2 \equiv 911 \bmod p$, so $x_2^2 \equiv 10y_2 \bmod p$. It turns out that $y_2 \bmod p$ has order 8. Also $c^4 \bmod p$ has order 8. Then

$$x_2^2 c^4 \equiv 10 y_2 c^4 \bmod p \Longrightarrow (x_2 c^2)^2 \equiv 10(y_2 c^4) \bmod p.$$

Set $x_3 = x_2 c^2 \equiv 334 \bmod p$ and $y_3 = y_2 c^4 \equiv 664 \bmod p$, so $x_3^2 \equiv 10y_3 \bmod p$. It turns out that $y_3 \bmod p$ has order 4. Also $c^8 \bmod p$ has order 4. Then

$$x_3^2 c^8 \equiv 10 y_3 c^8 \bmod p \Longrightarrow (x_3 c^4)^2 \equiv 10(y_3 c^8) \bmod p.$$

Set $x_4 = x_3 c^4 \equiv 482 \bmod p$ and $y_4 = y_3 c^8 \equiv 1 \bmod p$, so $x_4^2 \equiv 10 \bmod p$. We discovered that $482 \bmod p$ is a square root of $10 \bmod p$.

Using a different quadratic non-residue $b \bmod p$ in the Tonelli–Shanks algorithm may lead to another c, which may lead to the same or other solution of $x^2 \equiv 10 \bmod p$. See Exercise 6.3(b).

Example 6.2. When $p = 13$, we have $3 \equiv 4^2 \bmod 13$. Let's apply Tonelli–Shanks to $x^2 \equiv 3 \bmod p$ to see what solution we get. Set $a = 3$ and $p - 1 = 12 = 2^2 \cdot 3 = 2^e k$. Then $x_1 = a^{(k+1)/2} = 3^2 = 9$ and solving $x_1^2 \equiv 3y_1 \bmod p$ for y_1 leads to $y_1 \equiv 1 \bmod p$ (since $81 \equiv 3 \bmod 13$), so we're done: the Tonelli–Shanks algorithm led us us to $x \equiv 9 \equiv -4 \bmod p$, not $4 \bmod p$ and we never got to the step of needing a quadratic non-residue $b \bmod p$ at all.

Thus every quadratic non-residue $b \bmod 13$ "leads" to the same solution of $x^2 \equiv 3 \bmod 13$ in the Tonelli–Shanks algorithm for the simple reason that b is never used.

Here is a summary of the Tonelli–Shanks algorithm to solve $x^2 \equiv a \bmod p$ when $(\frac{a}{p}) = 1$:

Step 1: Write $p - 1 = 2^e k$ where $e \geq 1$ and k is odd. Set $x_1 = a^{(k+1)/2} \bmod p$. It has order dividing 2^{e-1}.

Step 2: Find b such that $(\frac{b}{p}) = -1$ and set $c = b^k \bmod p$, which has order 2^e, so $c^2 \bmod p$ has order 2^{e-1}.

Step 3: Set $y_1 = a^k \bmod p$, so $x_1^2 = y_1 a \bmod p$ and $y_1 \bmod p$ has order dividing 2^{e-1}.

Step 4: When $x_i^2 \equiv y_i a \bmod p$ and y_i has order 2^{j_i} dividing 2^{e-i} with $y_i \not\equiv 1 \bmod p$, multiply both sides by $(c^2)^{2^{e-1-j_i}}$, which also has order 2^{j_i}, so $x_{i+1}^2 \equiv y_{i+1} a \bmod p$ where $x_{i+1} \equiv x_i c^{2^{e-1-j_i}} \bmod p$ and $y_{i+1} \equiv y_i c^{2^{e-j_i} \bmod p}$. The order of $y_{i+1} \bmod p$ is $2^{j_{i+1}}$ where $0 \leq j_{i+1} < j_i$.

Step 5: When $x_i^2 \equiv y_i a \bmod p$ and $y_i \equiv 1 \bmod p$, a solution to $x^2 \equiv a \bmod p$ is $x = x_i$.

Since $y_1 = a^k \bmod p$ has order dividing 2^{e-1} and $c^2 \bmod p$ generates the unique subgroup of order 2^{e-1} in the cyclic group $(\mathbf{Z}/(p))^\times$, $y_1 \bmod p \in \langle c^2 \bmod p \rangle$. Writing $y_1 \equiv (c^2)^t = c^{2t} \bmod p$ for $t \in \mathbf{Z}$, $x_1^2 \equiv y_1 a \equiv c^{2t} a \bmod p$, so $(x_1 c^{-t})^2 \equiv a \bmod p$. The solution of $x^2 \equiv a \bmod p$ that comes from the Tonelli–Shanks algorithm is $x_1 c^{-t} = a^{(k+1)/2} c^{-t} \bmod p$ where $y_1 \equiv (c^2)^t \bmod p$. The steps in the Tonelli–Shanks algorithm are revealing the nonzero positions in the binary expansion of $t \bmod 2^{e-1}$ from the lowest to the highest positions.

Example 6.3. In Example 6.1 we want to solve $x^2 \equiv 10 \bmod 1249$ where $p - 1 = 1248 = 2^5 \cdot 39$ and $y_1 = 650 \bmod p$ and $c = 305 \bmod p$, so $c^2 \equiv 599 \bmod p$. The meaning of the different powers of $c^2 \bmod p$ that we used here can be seen by writing

$$1 \equiv y_4 \equiv y_3 c^8 \equiv y_2 c^4 c^8 \equiv y_1 c^2 c^4 c^8 \equiv y_1 c^{2+4+8} \equiv y_1 c^{14} \equiv y_1 (c^2)^7 \bmod p,$$

so $y_1 \equiv (c^2)^{-7} \bmod p$. HELP

In the Tonelli–Shanks algorithm, the only role of the quadratic non-residue $b \bmod p$ is to give us $c = b^k \bmod p$, which is guaranteed to have order 2^e (the highest power of 2 dividing $p - 1$). Once we have c, the number b no longer matters. Moreover, we can use the same c to solve $x^2 \equiv a \bmod p$ for each quadratic residue $a \bmod p$: c is independent of a.

Now we turn to a second algorithm to solve $x^2 \equiv a \bmod p$ when $(\frac{a}{p}) = 1$, due to Cipolla [1]. This algorithm uses a quadratic non-residue mod p, but in contrast to the Tonelli–Shanks algorithm, the quadratic non-residue used in Cipolla's algorithm to solve $x^2 \equiv a \bmod p$ depends on $a \bmod p$. Cipolla's algorithm also uses fields of order p^2, not just $\mathbf{Z}/(p)$.

We will need an $m \in \mathbf{Z}/(p)$ such that $m^2 - a \not\equiv \Box \bmod p$, namely $(\frac{m^2-a}{p}) = -1$. The next lemma shows nearly 50% of the numbers in $\mathbf{Z}/(p)$ fit that condition.

Lemma 6.4. *When p is an odd prime and $(\frac{a}{p}) = 1$, the set*

$$\left\{m \in \mathbf{Z}/(p) : \left(\frac{m^2 - a}{p}\right) = -1\right\}$$

has size $(p-1)/2$.

Proof. We will prove the complementary set $M = \{m \in \mathbf{Z}/(p) : (\frac{m^2-a}{p}) = 1\}$ in $\mathbf{Z}/(p)$ has size $(p+1)/2$.

Let

$$C = \{(x,y) \in \mathbf{Z}/(p) \times \mathbf{Z}/(p) : y^2 - a = x^2\} = \{(x,y) \in \mathbf{Z}/(p) \times \mathbf{Z}/(p) : y^2 - x^2 = a\}.$$

Since $y^2 - x^2 = (y+x)(y-x)$, the change of variables $u = y + x$ and $v = y - x$ (with inverse $x = (u-v)/2$ and $y = (u+v)/2$, which makes sense in $\mathbf{Z}/(p)$ since $p > 2$) makes C bijective with $\{(u,v) \in \mathbf{Z}/(p) \times \mathbf{Z}/(p) : uv = a\}$ and this last set has size $p-1$ since u is nonzero mod p and v is determined by u (and a).

The set M is the image of the projection $C \to \mathbf{Z}/(p)$ by $(x,y) \mapsto y$. To each number $y \in M$, how many points (x,y) are there in C? There's at least one (x,y) in C by the definition of M. When $y^2 = a$, x must be 0 so we have the single point $(0,y)$ in C. When $y^2 \neq a$, $y^2 - a \neq 0$, so it being a square mod p means it is a square in two ways: there are two x's such that $(x,y) \in C$. Thus

$$|C| = \sum_{y \in M} |\{x \in \mathbf{Z}/(p) : (x,y) \in C\}| = \sum_{\substack{y \in M \\ y^2 \neq a}} 2 + \sum_{\substack{y \in M \\ y^2 = a}} 1 = 2(|M| - 2) + 2 = 2|M| - 2,$$

so $|M| = (|C| + 2)/2 = (p+1)/2$. □

Since nearly 50% of m in $\mathbf{Z}/(p)$ satisfy $m^2 - a \not\equiv \Box \bmod p$, it is not hard in practice to find m by randomly picking m in $\mathbf{Z}/(p)$ and computing $(\frac{m^2-a}{p})$ by quadratic reciprocity until we find m where that Legendre symbol is -1.

Cipolla's algorithm solves $x^2 \equiv a \bmod p$ by using a quadratic non-residue of the form $m^2 - a \bmod p$ and a square root of it in a field bigger than $\mathbf{Z}/(p)$. Write $\mathbf{Z}/(p)$ as $\mathbf{F}_p$. When $(\frac{m^2-a}{p}) = -1$, the polynomial $x^2 - (m^2 - a)$ in $\mathbf{F}_p[x]$ is irreducible. Let r be a root of this polynomial in an extension of $\mathbf{F}_p$, so the field $\mathbf{F}_p(r)$ has order p^2: write this field as $\mathbf{F}_{p^2}$. We will find a square root of a in $\mathbf{F}_{p^2}$, and that square root must be in $\mathbf{F}_p$ itself when $(\frac{a}{p}) = 1$, since a number has at most two square roots in any field.

On the field $\mathbf{F}_{p^2}$, the pth power map is a field automorphism and $r^p \neq r$ since $r \notin \mathbf{F}_p$. Since r is a root of $x^2 - (m^2 - a)$, r^p is also a root and it is not r, so r^p is the other root, which is $-r$. Now we can write down a square root of a in $\mathbf{F}_{p^2}$: it is

$$s := (m + r)^{(p+1)/2}.$$

Let's check this works:

$$\begin{aligned} s^2 &= (m+r)^{p+1} \\ &= (m+r)(m+r)^p \\ &= (m+r)(m^p + r^p). \end{aligned}$$

Since $m \in \mathbf{F}_p$, $m^p = m$. We already indicated why $r^p = -r$. Thus

$$s^2 = (m+r)(m-r) = m^2 - r^2 = m^2 - (m^2 - a) = a.$$

Since a is a square in $\mathbf{F}_p$, the square root of it that we just found in $\mathbf{F}_{p^2}$ must be in $\mathbf{F}_p$.

What we just presented is Cipolla's algorithm. Here is a summary of it.

Step 1: for odd prime p and $a \in \mathbf{Z}/(p)$ such that $(\frac{a}{p}) = 1$, let $m \in \mathbf{Z}/(p)$ be chosen to satisfy $(\frac{m^2-a}{p}) = -1$.

Step 2: Let r be a square root of $m^2 - a$ in an extension field of $\mathbf{Z}/(p)$. Then $s^2 = a$ where $s := (m + r)^{(p+1)/2}$.

To make this algorithm computationally practical, view the field $\mathbf{F}_{p^2} = \mathbf{F}_p(r)$ as the quotient ring $\mathbf{F}_p[x]/(x^2 - (m^2 - a))$. Using this lets us express Cipolla's algorithm in the following concrete way.

Theorem 6.5. *When* $(\frac{a}{p}) = 1$ *and* $m \in \mathbf{Z}/(p)$ *satisfies* $(\frac{m^2-a}{p}) = -1$*,* $a \bmod p$ *has square root* $(m + x)^{(p+1)/2}$ *in* $\mathbf{F}_p[x]/(x^2 - (m^2 - a))$*.*

Proof. Use $\mathbf{F}_p[x]/(x^2 - (m^2 - a))$ as the model of $\mathbf{F}_{p^2}$ in the above calculations, where we can use $r = x \bmod (x^2 - (m^2 - a))$ since $x^2 \equiv m^2 - a \bmod (x^2 - (m^2 - a))$. □

Example 6.6. Let $p = 41$. By quadratic reciprocity, $(\frac{2}{p}) = 1$. To solve $x^2 \equiv 2 \bmod p$ by Cipolla's algorithm, check when $m = 3$ that $m^2 - 2 = 7$ is a quadratic non-residue mod p. Since $(p + 1)/2 = 21$, in the field $\mathbf{F}_p[x]/(x^2 - 7)$ Cipolla's algorithm says $(3 + x)^{21}$ squares to 2. With a computer, $(3+x)^{21} = 17$ in $\mathbf{F}_p[x]/(x^2 - 7)$, and indeed $17^2 = 289 \equiv 2 \bmod 41$.

Exercises.

1. If G is a nontrivial cyclic 2-group and x and y in G have the same order 2^r, then prove xy has order dividing 2^{r-1}. This applies in particular to two generators of G.
2. The number 593 is prime. Show $(\frac{17}{593}) = 1$ and use the Tonelli–Shanks algorithm to solve $x^2 \equiv 17 \bmod 593$ using the quadratic non-residue 3 mod 593.
3. The number 1249 is prime.
   a) Show $(\frac{3}{1249}) = 1$ and solve $x^2 \equiv 3 \bmod 593$ by the Tonelli–Shanks algorithm using the quadratic non-residue 7 mod 1249.
   b) Solve $x^2 \equiv 10 \bmod 1249$ by the Tonelli–Shanks algorithm five times using each of the quadratic non-residues 7, 11, 21, 23, and 29 mod 1249. Sometimes you'll get the solution 482 mod 1249 and sometimes you'll get $767 \equiv -482 \bmod 1249$.
4. Example 6.6 solved $x^2 \equiv 2 \bmod 41$ using Cipolla's algorithm with $m = 3$. Check that Cipolla's algorithm to solve $x^2 \equiv 2 \bmod 41$ can also use $m = 4$, 6, and 7. In each case, check whether the algorithm leads to the same solution of $x^2 \equiv 2 \bmod 41$ as in Example 6.6. (Answer: it does when $m = 4$ and 6, but not when $m = 7$.)
5. Write a computer program that carries out the Tonelli–Shanks algorithm. Make sure to check first that the modulus p in the congruence is prime.
6. In Lemma 6.4, show $\{m \in \mathbf{Z}/(p) : (\frac{m^2-a}{p}) = -1\}$ has size $(p+1)/2$ when $(\frac{a}{p}) = -1$.
7. What happens if you run the Tonelli–Shanks algorithm or Cipolla's algorithm to solve $x^2 \equiv a \bmod p$ in case $a \not\equiv \square \bmod p$?

7. Quadratic reciprocity and division rings

For nonzero $a \in \mathbf{Z}$, what can be said about how often $(\frac{a}{p})$ is 1 or -1?

(1) If $a = \square$ in $\mathbf{Z}$, then $(\frac{a}{p}) = 1$ for all p not dividing $2a$.
(2) If $a \neq \square$ in $\mathbf{Z}$, then $(\frac{a}{p}) = 1$ for infinitely many p. This is a special case of a general theorem: when $f(x)$ is nonconstant in $\mathbf{Z}[x]$, there are infinitely many primes p such that $f(x) \equiv 0 \bmod p$ has a solution. See `https://math.stackexchange.com/questions/1019538`. This does not need quadratic reciprocity.
(3) If $a \neq \square$ in $\mathbf{Z}$, then $(\frac{a}{p}) = -1$ for infinitely many p. See [2, Theorem 3, p. 57], which is a proof using quadratic reciprocity. The case $a = -1$ is part of Theorem 3.1.

Using quadratic reciprocity and Dirichlet's theorem on primes in arithmetic progression, when $a \neq \Box$ the two sets of primes $\{p : (\frac{a}{p}) = 1\}$ and $\{p : (\frac{a}{p}) = -1\}$ are not only infinite, but also each has density 1/2 within the set of all primes.

That $\{(p : (\frac{a}{p}) = -1\}$ is infinite when $a \neq \Box$ has an application to division rings. What's a division ring? In short, it is a possibly noncommutative field. That is, division rings are defined just like fields except we don't insist that multiplication is commutative. The nonzero elements in a division ring are a posssibly noncommutative group under multiplication, so a nonzero element's multiplicative inverse on the left and right sides are the same (a general property of all groups).

Example 7.1. The most basic example of a noncommutative division ring is Hamilton's quaternions, which is the 4-dimensional **R**-vector space

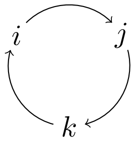
$$\mathbf{H} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$$

where multiplication is defined so that real numbers commute with i, j, and k and

- $i^2 = j^2 = k^2 = -1$,
- $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, and $ik = -j$.

All of these multiplication rules among i, j, and k are consequences of the four conditions $i^2 = -1$, $j^2 = -1$, $ij = k$, and $ji = -k$. The only quaternions that commute with all quaternions are the real numbers so that, borrowing a term from group theory, we say **R** is the *center* of **H**.

To remember the rules for multiplying i, j, and k by each other, put them in alphabetical order around a circle as below. Products following this order get a plus sign, and products going against the order get a minus sign, *e.g.*, $jk = i$ and $ik = -j$.



When $q = x + yi + zj + wk$, its *conjugate* is $\overline{q} = x - yi - zj - wk$, and we set the *norm* of q to be

$$\mathrm{N}(q) = q\overline{q} = \overline{q}q = x^2 + y^2 + z^2 + w^2 \geq 0.$$

When $q \neq 0$, so some coefficient of q is nonzero, $\mathrm{N}(q)$ is a positive real number and q has multiplicative inverse $\overline{q}/\mathrm{N}(q)$.

The division ring **H** can be written not only as a 4-dimensional real vector space, but as a two-dimensional (left) complex vector space:

$$\mathbf{H} = (\mathbf{R} + \mathbf{R}i) + (\mathbf{R} + \mathbf{R}i)j = \mathbf{C} + \mathbf{C}j \tag{7.1}$$

where $j^2 = -1$ and $jz = \overline{z}j$ for all $z \in \mathbf{C}$.

Example 7.2. There are no finite examples of noncommutative division rings: Wedderburn proved all finite division rings are commutative.

Although **H** was discovered by Hamilton in 1843 somewhat accidentally (he had been trying to extend multiplication among complex numbers from **C** to $\mathbf{R}^3$), Frobenius proved 35 years later that they have a special role in algebra.

Theorem 7.3 (Frobenius, 1878)**.** *The only noncommutative* $\mathbf{R}$*-central*[6] *division ring that is finite-dimensional over* $\mathbf{R}$ *is* $\mathbf{H}$*.*

The following definition generalizes the description of $\mathbf{H}$ to rings that are 4-dimensional over their center, which can be any field not of characteristic 2.

Definition 7.4. Let F be a field not of characteristic 2. A *quaternion algebra* over F is a 4-dimensional F-vector space

$$F + Fi + Fj + Fk$$

where multiplication is defined so that elements of F commute with i, j, and k and

- $i^2 = a \in F^\times$, $j^2 = b \in F^\times$,
- $k = ij = -ji$.

This ring is denoted $(a,b)_F$. It is noncommutative since $ij \neq ji$: $ij - ji = 2ij$, which is not 0 since 2, i, and j are all units (F does not have characteristic 2). The elements of $(a,b)_F$ that commute with all of $(a,b)_F$ are the elements of F, so $(a,b)_F$ has center F.

All products among i, j, and k can be worked out from the rules in the definition, *e.g.*, $k^2 = kk = ijij = ij(-ji) = -ij^2i = -ibi = -i^2b = -ab$ and $jk = jij = -ijj = -bi$.

Example 7.5. The Hamilton quaternions $\mathbf{H}$ is the quaternion algebra $(-1,-1)_{\mathbf{R}}$.

Example 7.6. Taking $F = \mathbf{Q}$, $a = 2$, and $b = 5$,

$$(2,5)_{\mathbf{Q}} = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$$

where $i^2 = 2$, $j^2 = 5$, and $k = ij = -ji$, so $k^2 = -(2)(5) = -10$. In analogy to (7.1),

$$(2,5)_{\mathbf{Q}} = (\mathbf{Q} + \mathbf{Q}i) + (\mathbf{Q} + \mathbf{Q}i)j = \mathbf{Q}(\sqrt{2}) + \mathbf{Q}(\sqrt{2})j \tag{7.2}$$

where $j^2 = 5$ and $j\alpha = \overline{\alpha}j$ for all $\alpha \in \mathbf{Q}(\sqrt{2})$. So the ring $(2,5)_{\mathbf{Q}}$ contains $\mathbf{Q}(\sqrt{2})$ as a subfield.

Both (7.1) and (7.2) extend to quaternion algebras $(a,b)_F$ where $a \neq \square$ in F:

$$(a,b)_F = (F + Fi) + (F + Fi)j = F(\sqrt{a}) + F(\sqrt{a})j \tag{7.3}$$

where $j^2 = b$ and $j\alpha = \overline{\alpha}$ for all $\alpha \in F(\sqrt{a})$

Here are three general properties of quaternion algebras. Proofs of the 2nd and 3rd properties can be read in Theorems 4.3 and 4.20 in https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf.

1. $(a,b)_F \cong (b,a)_F$ for all a and b in $F^\times$,
2. $(a,1)_F \cong \mathrm{M}_2(F)$,
3. If $(a,b)_F \not\cong \mathrm{M}_2(F)$ then $(a,b)_F$ is a division ring.

Now we will focus on quaternion algebras over $\mathbf{Q}$. Legendre symbols that equal -1 always lead to 4-dimensional division rings over $\mathbf{Q}$.

Theorem 7.7. *If* $a \in \mathbf{Z} - \{0\}$ *and* p *is an odd prime, then*

$$\left(\frac{a}{p}\right) = -1 \Longrightarrow (a,p)_{\mathbf{Q}} \text{ is a division ring.}$$

Proof. This is proved as Theorem 3.9 in https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf. □

[6] An *F-central division ring* means a division ring with center F. It is commutative only when it is F.

Example 7.8. The quaternion algebra $(2,5)_{\mathbf{Q}}$ is a division ring since $(\frac{2}{5}) = -1$.

Example 7.9. Is $(3,11)_{\mathbf{Q}}$ a division ring? Since $(\frac{3}{11}) = 1$, it appears we can't use Theorem 7.7, but $(3,11)_{\mathbf{Q}} \cong (11,3)_{\mathbf{Q}}$ and $(\frac{11}{3}) = -1$, so we can use Theorem 7.7 with $a = 11$ and $b = 3$ to see that $(3,11)_{\mathbf{Q}}$ is a division ring.

Example 7.10. When p and q are distinct odd primes, $(p,q)_{\mathbf{Q}}$ is a division ring if and only if $(\frac{p}{q}) = -1$ or $(\frac{q}{p}) = -1$. The "only if" direction is not obvious.

Theorem 7.11. *If $a \in \mathbf{Z} - \{0\}$ and p and q are distinct odd primes, then $(a,p)_{\mathbf{Q}}$ and $(a,q)_{\mathbf{Q}}$ are nonisomorphic division rings.*

Proof. The case $a = -1$ is Corollary 5.5 in https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf. The proof when $a = -1$ has all the key ideas needed to prove the general case. □

Theorems 7.7 and 7.11 tell us there are *infinitely many* $\mathbf{Q}$-central division rings with dimension 4 by using $(a,p)_{\mathbf{Q}}$ where a is a fixed nonsquare in $\mathbf{Z}$ and p runs over the odd primes such that $(\frac{a}{p}) = -1$. Moreover, since each quadratic field K is $\mathbf{Q}(\sqrt{a})$ for some nonsquare integer a and $\mathbf{Q}(\sqrt{a})$ is contained in $(a,p)_{\mathbf{Q}}$ by (7.3), there are infinitely many $\mathbf{Q}$-central division rings with dimension 4 that contain a specified quadratic field K.

We end this section with some remarks about division rings with center equal to the p-adic numbers $\mathbf{Q}_p$. While there is only one noncommutative finite-dimensional $\mathbf{R}$-central division ring by Theorem **??**, there are many $\mathbf{Q}_p$-central division rings, but (i) there are only finitely many with each dimension (which includes no examples in some dimensions) and (ii) there is only one example with dimension 4. So when we look in dimension 4, the situations over $\mathbf{R}$ and $\mathbf{Q}_p$ look the same and both are unlike $\mathbf{Q}$. When $p = 2$, the unique $\mathbf{Q}_2$-central division ring with dimension 4 is $\mathbf{H}(\mathbf{Q}_2)$, the quaternions with $\mathbf{Q}_2$-coefficients. When $p \neq 2$, the unique $\mathbf{Q}_p$-central division ring with dimension 4 is *not* $\mathbf{H}(\mathbf{Q}_p)$, which is isomorphic to the 2×2 matrix ring $\mathrm{M}_2(\mathbf{Q}_p)$ and that is not a division ring. Instead, the quaternion algebra $(a,p)_{\mathbf{Q}_p}$ is a division ring when $a \in \mathbf{Z}$ is not a square mod p.

Exercises.

1. In $(a,b)_F = F + Fi + Fj + Fk$, show $ik = -ki = aj$, $kj = -jk = bi$, and $jk = -kj = -bi$. and $(a,b)_F$ has center F.
2. For $q \in (a,b)_F$, define the conjugate of $q = x+yi+zj+wk$ to be $\overline{q} = x-yi-zj-wk$.
   a) Show $q\overline{q} = \overline{q}q = x^2 - ay^2 - bz^2 + abw^2 \in F$. This is called the norm of q and is denoted $\mathrm{N}(q)$, so when $\mathrm{N}(q) \in F^\times$, q has inverse $\overline{q}/\mathrm{N}(q)$.
   b) Show $\overline{q_1q_2} = \overline{q_2}\,\overline{q_1}$ for all q_1 and q_2 in $(a,b)_F$.
3. When b is a square in $F^\times$, say $b = c^2$, show $(a,b)_F \cong \mathrm{M}_2(F)$ as rings by
$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & -c \\ ac & 0 \end{pmatrix}$$
   and extend this to all of $(a,b)_F$ by F-linearity. The matrix that k maps to is the product of the matrices that i and j map to (in that order).

8. Quadratic reciprocity in $\mathbf{Z}[i]$

We saw in Theorems 5.1 and 5.4 that if d is an integer that is not a square and $\mathbf{Z}[\sqrt{d}]$ has unique factorization, then for all primes p,

$$d \equiv \Box \bmod p \Longleftrightarrow \pm p = x^2 - dy^2 \bmod p \text{ for some } x, y \in \mathbf{Z}.$$

The reasoning in the proofs of Theorem 5.4 and Corollary 5.5 go through with $\mathbf{Z}$ replaced by $\mathbf{Z}[i]$, leading to the next theorem.

Theorem 8.1. *Let δ in $\mathbf{Z}[i]$ not be a square. If $\mathbf{Z}[i][\sqrt{\delta}]$ has unique factorization then for all primes π in $\mathbf{Z}[i]$,*

$$\delta \equiv \Box \bmod \pi \Longleftrightarrow u\pi = x^2 - \delta y^2 \textit{ for some } x, y \in \mathbf{Z}[i] \textit{ and unit } u \in \mathbf{Z}[i]^\times. \tag{8.1}$$

If $i = x^2 - \delta y^2$ for some $x, y \in \mathbf{Z}[i]$, then $u\pi$ can be replaced by π on the right side of the equivalence.

Proof. It's left to the reader to prove (8.1). When $i = x^2 - \delta y^2$ in $\mathbf{Z}[i]$, also powers of i have that form by multiplicativity of the norm map $\mathbf{Z}[i][\sqrt{\delta}] \to \mathbf{Z}[i]$ where $x + y\sqrt{\delta} \mapsto x^2 - \delta y^2$, so being able to write $u\pi$ as $x^2 - \delta y^2$ in $\mathbf{Z}[i]$ implies π itself has that form. $\Box$

Example 8.2. It can be shown that $\mathbf{Z}[i][\sqrt{1+i}] = \mathbf{Z}[\sqrt{1+i}]$ has unique factorization, and $i = x^2 - (1+i)y^2$ when $x = i$ and $y = i$, so for all primes π in $\mathbf{Z}[i]$,

$$1 + i \equiv \Box \bmod \pi \Longleftrightarrow \pi = x^2 - (1+i)y^2 \textit{ for some } x, y \in \mathbf{Z}[i].$$

Taking $\pi = 2 + i$, we have $1 + i \equiv 4 \bmod \pi$, so we can write $2 + i = x^2 - (1+i)y^2$ for some x and y in $\mathbf{Z}[i]$. A search yields the solution $x = 3$ and $y = 2 - i$.

To make the condition $\delta \equiv \Box \bmod \pi$ explicit in terms of π we can use quadratic reciprocity in $\mathbf{Z}[i]$. Every prime in $\mathbf{Z}[i]$ divides a prime number in $\mathbf{Z}$, and up to unit multiple the only prime in $\mathbf{Z}[i]$ that divides 2 is $1+i$ since $2 = (1+i)(1-i) = (1+i)(-i)(1+i) = -i(1+i)^2$. Primes in $\mathbf{Z}[i]$ dividing odd prime numbers are called *odd*. Examples of odd primes in $\mathbf{Z}[i]$ include $2 + i$, $2 - i$, 3, 7, and $2 + 3i$. More generally, Gaussian integers α that are not divisible by $1 + i$ are called odd, and this condition is equivalent to $\mathrm{N}(\alpha)$ being odd in $\mathbf{Z}$.

When π is an odd prime in $\mathbf{Z}[i]$ and $\alpha \in \mathbf{Z}[i]$, the Legendre symbol $(\frac{\alpha}{\pi})$ is defined by

$$\left(\frac{\alpha}{\pi}\right) = \begin{cases} 1, & \text{if } \alpha \equiv \Box \bmod \pi, \alpha \not\equiv 0 \bmod \pi, \\ -1, & \text{if } \alpha \not\equiv \Box \bmod \pi, \\ 0, & \text{if } \alpha \equiv 0 \bmod \pi. \end{cases}$$

Example 8.3. The number $2+3i$ is prime in $\mathbf{Z}[i]$ with $\mathrm{N}(2+3i) = 13$, and $2+3x \equiv 0 \bmod 13$ has solution $x = 8$, so $\mathbf{Z}[i]/(2+3i) \cong \mathbf{Z}/(13)$ by mapping $a+bi \bmod 2+3i$ to $a+8b \bmod 13$. To determine $(\frac{a+bi}{2+3i})$ in $\mathbf{Z}[i]$ is the same as determining $(\frac{a+8b}{13})$ in $\mathbf{Z}$. Thus $(\frac{1+i}{2+3i}) = (\frac{9}{13}) = 1$ and $(\frac{i}{2+3i}) = (\frac{8}{13}) = (\frac{2}{13}) = -1$. That shows $1 + i \equiv 3^2 \bmod 2 + 3i$ and $i \not\equiv \Box \bmod 2 + 3i$.

It is easy to by the definition of $(\frac{\alpha}{\pi})$ that $\alpha \equiv \beta \bmod \pi \Longrightarrow (\frac{\alpha}{\pi}) = (\frac{\beta}{\pi})$. Euler's criterion for the Legendre symbol on $\mathbf{Z}$ carries over to $\mathbf{Z}[i]$: for odd primes π in $\mathbf{Z}[i]$ and $\alpha \in \mathbf{Z}[i]$,

$$\left(\frac{\alpha}{\pi}\right) \equiv \alpha^{(\mathrm{N}(\pi)-1)/2} \bmod \pi, \tag{8.2}$$

which implies the multiplicativity of the Legendre symbol on $\mathbf{Z}[i]$: for odd primes π in $\mathbf{Z}[i]$ and arbitrary α and β in $\mathbf{Z}[i]$,

$$\left(\frac{\alpha\beta}{\pi}\right) = \left(\frac{\alpha}{\pi}\right)\left(\frac{\beta}{\pi}\right). \tag{8.3}$$

This reduces the calculation of $(\frac{\alpha}{\pi})$ to the case when α is an odd prime, i, or $1+i$.

To present the quadratic reciprocity law in $\mathbf{Z}[i]$, we will use a normalization of the odd Gaussian integers that singles out a choice among the 4 unit multiples of each such Gaussian integer. This is analogous to the way quadratic reciprocity in $\mathbf{Z}$ uses *positive* primes. To appreciate this point, notice that in $\mathbf{Z}$ the prime p in $(\frac{a}{p})$ plays the role of a modulus, so we could let p be a negative prime without affecting a Legendre symbol's value: $a \equiv \Box \bmod p\mathbf{Z}$ is the same thing as $a \equiv \Box \bmod (-p)\mathbf{Z}$. Thus $(\frac{2}{-5}) = (\frac{2}{5}) = -1$ and $(\frac{2}{-7}) = (\frac{2}{7}) = 1$. The rule $(\frac{-1}{p}) = (-1)^{(p-1)/2}$, however, is not true when $p < 0$, *e.g.*, $(\frac{-1}{-3}) = (\frac{-1}{3}) = -1$ while $(-1)^{(-3-1)/2} = 1$, and $(\frac{-1}{-5}) = (\frac{-1}{5}) = 1$ while $(-1)^{(-5-1)/2} = -1$. Similarly, the factor $(-1)^{(p-1)/2\cdot(q-1)/2}$ in the main law of quadratic reciprocity in $\mathbf{Z}$ is not always correct if we let p or q be negative. Every odd prime in $\mathbf{Z}$ is $\pm 1 \bmod 4$, so all odd primes in $\mathbf{Z}$ can be made 1 mod 4 by multiplying them by a suitable sign, and Exercise 8.2 shows how quadratic reciprocity in $\mathbf{Z}$ looks on positive and negative odd primes that are both 1 mod 4.

To normalize odd Gaussian integers in $\mathbf{Z}[i]$, the units ± 1 and $\pm i$ and also $\mathbf{Z}[i]/(1+i)^3 = \mathbf{Z}[i]/(2+2i)$ has 4 units that are represented by ± 1 and $\pm i \bmod 2+2i$. Thus when α is odd in $\mathbf{Z}[i]$, there is a unique $u \in \{\pm 1, \pm i\}$ such that $\alpha \equiv u \bmod 2+2i$, so $u^{-1}\alpha \equiv 1 \bmod 2+2i$. Each odd α has a unique unit multiple that is $1 \bmod 2+2i$. When $\alpha \equiv 1 \bmod 2+2i$, call α *normalized.*

Example 8.4. We have $1+2i \equiv -1 \bmod 2+2i$, so $-(1+2i) \equiv 1 \bmod 2+2i$.

Example 8.5. We have $2-3i \equiv -i \bmod 2+2i$, so $i(2-3i) \equiv 1 \bmod 2+2i$.

Two normalized odd Gaussian integers are not unit multiples of each other unless they are equal, just like positive integers are not unit multiples of each other in $\mathbf{Z}$ unless they are equal.

Here is one way to formulate quadratic reciprocity in $\mathbf{Z}[i]$. Note Gaussian integers that are $1 \bmod 2+2i$ are 1 or $3+2i \bmod 4$ and are $1, 5, 3+2i$, or $7+2i \bmod 4(1+i)$. This is like saying integers that are 1 mod 4 are 1 or 5 mod 8 and are $1, 5, 9$, or 13 mod 16.

Theorem 8.6. *Let π be a normalized odd prime in $\mathbf{Z}[i]$. For a normalized odd prime π' in $\mathbf{Z}[i]$ that is not equal to π,*

$$\left(\frac{\pi'}{\pi}\right) = \left(\frac{\pi}{\pi'}\right) \tag{8.4}$$

and

$$\left(\frac{i}{\pi}\right) = \begin{cases} 1, & \textit{if } \pi \equiv 1 \bmod 4\mathbf{Z}[i], \\ -1, & \textit{if } \pi \equiv 3+2i \bmod 4\mathbf{Z}[i] \end{cases} \tag{8.5}$$

and

$$\left(\frac{1+i}{\pi}\right) = \begin{cases} 1, & \textit{if } \pi \equiv 1, 7+2i \bmod 4(1+i)\mathbf{Z}[i], \\ -1, & \textit{if } \pi \equiv 5, 3+2i \bmod 4(1+i)\mathbf{Z}[i]. \end{cases} \tag{8.6}$$

We call (8.4) the main law of quadratic reciprocity in $\mathbf{Z}[i]$ and (8.5) and (8.6) the supplementary laws of quadratic reciprocity for $\mathbf{Z}[i]$. In $\mathbf{Z}$, the main law linking $(\frac{p}{q})$ and $(\frac{q}{p})$ for positive primes depends on $p \bmod 4$ and $q \bmod 4$ and the supplementary law for $(\frac{-1}{p})$ depends on $p \bmod 4$, while the supplementary law for $(\frac{2}{p})$ depends on $p \bmod 8$. In $\mathbf{Z}[i]$, the supplementary law for $(\frac{i}{\pi})$ depends on $\pi \bmod 4\mathbf{Z}[i]$, while the supplementary law for $(\frac{1+i}{\pi})$ depends on $\pi \bmod 4(1+i)\mathbf{Z}[i]$. If we had expressed quadratic reciprocity in $\mathbf{Z}[i]$ for all odd primes, not just normalized odd primes, then we'd see that the main law depends on the odd primes mod $4\mathbf{Z}[i]$.

The supplementary law for $(\frac{i}{\pi})$ is a simple consequence of Euler's criterion (8.2), just as the supplementary law for $(\frac{-1}{p})$ is in $\mathbf{Z}$: see Exercise 8.3. Proofs of the main law and the supplementary law for $(\frac{1+i}{\pi})$ in Theorem 8.6 are omitted. You could look at the *quartic* reciprocity law in [2, Theorem 2, p. 123] and [2, Exer. 37, Chap. 9] and square them, since the square of the quartic residue symbol in $\mathbf{Z}[i]$ is the Legendre symbol in $\mathbf{Z}[i]$. Note that in [2] odd Gaussian integers that are 1 mod $2+2i$ are called "primary" rather than normalized.

Example 8.7. We will determine whether $3-i \equiv \Box \bmod 1+6i$ by computing $(\frac{3-i}{1+6i})$. The number $1+6i$ is prime in $\mathbf{Z}[i]$ since its norm 37 is prime in $\mathbf{Z}$, but $1+6i$ is not normalized: $1+6i \equiv -1 \bmod 2+2i$. The number $3-i$ is reducible: its norm is 10 and it factors as $(1+i)(1-2i)$, where the Gaussian prime $1-2i$ is not normalized: $1-2i \equiv -1 \bmod 2+2i$. To express $3-i$ as a product of a unit, $1+i$, and a normalized prime, write

$$3-i = (1+i)(1-2i) = (1+i)(-1+2i)(-1) = (1+i)(-1+2i)i^2,$$

so

$$\left(\frac{3-i}{1+6i}\right) = \left(\frac{3-i}{-1-6i}\right) = \left(\frac{1+i}{-1-6i}\right)\left(\frac{-1+2i}{-1-6i}\right).$$

Since $-1-6i$ is normalized and $-1-6i \equiv 7+2i \bmod 2+2i$, $(\frac{1+i}{-1-6i}) = 1$ by the supplementary law for $(\frac{1+i}{\pi})$. Since $-1+2i$ and $-1-6i$ are normalized, by the main law

$$\left(\frac{-1+2i}{-1-6i}\right) = \left(\frac{-1-6i}{-1+2i}\right)$$

and $1-6i \equiv -4 \bmod -1+2i$, so

$$\left(\frac{3-i}{1+6i}\right) = \left(\frac{-1+2i}{-1-6i}\right) = \left(\frac{-1-6i}{-1+2i}\right) = \left(\frac{-4}{-1+2i}\right) = \left(\frac{(2i)^2}{-1+2i}\right) = 1.$$

Thus $3-i \equiv \Box \bmod 1+6i$. Explicitly, $3-i \equiv (2-3i)^2 \bmod 1+6i$, but the quadratic reciprocity law in $\mathbf{Z}[i]$ does not tell us that square root.

Example 8.8. Returning to Example 8.2, when π is a *normalized* odd prime the supplementary law for $(\frac{1+i}{\pi})$ tells us that

$$\pi = x^2 - (1+i)y^2 \text{ for some } x, y \in \mathbf{Z}[i] \iff \pi \equiv 1, 7+2i \bmod 4(1+i).$$

Take $\pi = 2+i$ as in Example 8.2: π is not normalized, but $i\pi = -1+2i$ is normalized and $-1+2i \equiv 7+2i \bmod 4+4i$, so we can write $i\pi$ as $x^2-(1+i)y^2$ in $\mathbf{Z}[i]$ and thus also we can write π as $x^2-(1+i)y^2$ in $\mathbf{Z}[i]$ since the unit i is an $x^2-(1+i)y^2$ in $\mathbf{Z}[i]$. This approach based on quadratic reciprocity in $\mathbf{Z}[i]$ does not require us to explicitly determine how $1+i \bmod \pi$ is a square as we did in Example 8.2.

Exercises.

1. Prove (8.2) and (8.3) by reasoning analogous to proofs in $\mathbf{Z}$.
2. When p and q are primes in $\mathbf{Z}$ that may be negative but are both 1 mod 4, show
$$\left(\frac{q}{p}\right) = (-1)^{(|p|-1)/2\cdot(|q|-1)/2}\left(\frac{p}{q}\right).$$
For example, taking $p = -7$ and $q = -3$,
$$\left(\frac{-3}{-7}\right) = \left(\frac{-3}{7}\right) = \left(\frac{4}{7}\right) = 1$$
and
$$(-1)^{(|p|-1)/2\cdot(|q|-1)/2}\left(\frac{q}{p}\right) = (-1)^{(3-1)/2\cdot(7-1)/2}\left(\frac{-7}{-3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1.$$
3. Use Euler's criterion (8.2) to show $(\frac{i}{\pi}) = i^{(\mathrm{N}(\pi)-1)/2}$ in $\mathbf{Z}[i]$. (Hint: ± 1 and $\pm i$ are incongruent modulo $2+2i$.) Take cases when $\pi \equiv 1$ and $3+2i \bmod 4\mathbf{Z}[i]$ to show in the first case that $(\frac{i}{\pi}) = 1$ and in the second case $(\frac{i}{\pi}) = -1$. Keep in mind that i^m for $m \in \mathbf{Z}$ only depends on $m \bmod 4$.
4. By Example 8.3, $1+i \equiv \square \bmod 2+3i$. Find x and y in $\mathbf{Z}[i]$ such that $x^2-(1+i)y^2 = 2+3i$.
5. A square root of i is $\pm\zeta_8$, where ζ_8 is a root of unity of order 8.

   a) It turns out that $\mathbf{Z}[i][\sqrt{i}] = \mathbf{Z}[\zeta_8]$ has unique factorization. Use this to show for all primes π in $\mathbf{Z}[i]$ that
$$i \equiv \square \bmod \pi \Longleftrightarrow \pi = x^2 - iy^2 \bmod p \textit{ for some } x, y \in \mathbf{Z}[i].$$
(Hint: show $i = x^2 - iy^2$ in $\mathbf{Z}[i]$ in order to avoid having $u\pi$ on the right side with an ambiguous unit u.

   b) Show $i \equiv \square \bmod 3\mathbf{Z}[i]$ and solve $x^2 - iy^2 = 3$ in $\mathbf{Z}[i]$.

   c) Show $i \equiv \square \bmod (4+5i)\mathbf{Z}[i]$ and solve $x^2 - iy^2 = 4+5i$ in $\mathbf{Z}[i]$
6. Use quadratic reciprocity in $\mathbf{Z}[i]$ to show $(\frac{4+i}{2+5i}) = -1$. (Hint: neither $4+i$ nor $2+5i$ is normalized, so first find unit multiples of these Gaussian primes that are normalized.)

References

[1] M. Cipolla, "Un metodo per la risoluzione della congruenza di secondo grado," Rend. Accad. Sci. Fis. Mat. Napoli **9** (1903), 154–163. URL https://babel.hathitrust.org/cgi/pt?id=coo.31924070554898&seq=158.

[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[3] V. A. Lebesgue, "Remarques diverses sur les nombres premiers," Nouv. Annales Math. **15** (1856), 130–134. URL http://www.numdam.org/item/ NAM_1856_1_15__130_0.pdf

[4] L. J. Mordell, "A Statement by Fermat," Proceedings of the London Math. Soc. **18** (1920), v-vi.

[5] L. J. Mordell, "A Chapter in the Theory of Numbers," Cambridge Univ. Press, 1947.

[6] L. J. Mordell, "Two Papers on Number Theory," VEB Deutscher Verlag der Wissenschaften, Berlin, 1972.

[7] D. Shanks, Five number-theoretic algorithms, pp. 51–70 in "Proceedings of the Second Manitoba Conference on Numerical Mathematics," Congressus Numerantium, *Utilitas Math.* **7** (1973).

[8] A. Tonelli, "Bemerkung über die Auflösung quadratischer Congruenzen," Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen (1891), 344–346. URL https://eudml.org/doc/180329.