1. Do:

(a) Calculate the cubic residue symbols $\left[\frac{4+\sqrt{-3}}{11}\right]_3$, $\left[\frac{2\sqrt{-3}}{4+\sqrt{-3}}\right]_3$, and $\left[\frac{2+\sqrt{-3}}{7+2\sqrt{-3}}\right]_3$. Which elements are cubic residues and which are not?

- We have $\left[\frac{4+\sqrt{-3}}{11}\right]_3 \equiv (4+\sqrt{-3})^{(N(11)-1)/3} = (4+\sqrt{-3})^{40} \equiv \omega^2 \pmod{11}$ so $\left[\frac{4+\sqrt{-3}}{11}\right]_3 = \boxed{\omega^2}$. Thus $4+\sqrt{-3}$ $\boxed{\text{is not a cubic residue}}$ modulo 11.
- Also $\left[\frac{2\sqrt{-3}}{4+\sqrt{-3}}\right]_3 \equiv (2\sqrt{-3})^{(N(4+\sqrt{-3})-1)/3} = (2\sqrt{-3})^6 \equiv 1 \pmod{4+\sqrt{-3}}$ so $\left[\frac{2\sqrt{-3}}{4+\sqrt{-3}}\right]_3 = \boxed{1}$. Thus $2\sqrt{-3}$ $\boxed{\text{is a cubic residue}}$ modulo $4+\sqrt{-3}$.
- Finally $\left[\frac{2+\sqrt{-3}}{7+2\sqrt{-3}}\right]_3 \equiv (2+\sqrt{-3})^{(N(7+2\sqrt{-3})-1)/3} = (2+\sqrt{-3})^{20} \equiv \omega \pmod{7+2\sqrt{-3}}$ so $\left[\frac{2+\sqrt{-3}}{7+2\sqrt{-3}}\right]_3 = \boxed{\omega}$. Thus $2+\sqrt{-3}$ $\boxed{\text{is not a cubic residue}}$ modulo $7+2\sqrt{-3}$.

(b) Find the primary associates of the primes $2+\sqrt{-3}$ and $7+2\sqrt{-3}$ in $\mathcal{O}_{\sqrt{-3}}$, and then verify cubic reciprocity for these associates.

- Since $2+\sqrt{-3} = 3+2\omega$, we see that $-\omega^2(2+\sqrt{-3}) = \boxed{-1-3\omega}$ is primary. Likewise, since $7+2\sqrt{-3} = 9+4\omega$ we see that $-\omega^2(7+2\sqrt{-3}) = \boxed{5+9\omega}$ is primary.
- Then $\left[\frac{-1-3\omega}{5+9\omega}\right]_3 \equiv (-1-3\omega)^{(N(5+9\omega)-1)/3} \equiv (-1-3\omega)^{20} \equiv \omega^2 \pmod{9+5\omega}$.
- Also, $\left[\frac{5+9\omega}{-1-3\omega}\right]_3 \equiv (5+9\omega)^{(N(-1-3\omega)-1)/3} \equiv (5+9\omega)^2 \equiv \omega^2 \pmod{-1-3\omega}$.
- These are equal, as cubic reciprocity dictates they should be.

(c) Calculate the quartic residue symbols $\left[\frac{5+i}{7}\right]_4$, $\left[\frac{2i}{6+i}\right]_4$, and $\left[\frac{-2+i}{7-2i}\right]_4$. Which elements are quartic residues? Which elements are quadratic residues?

- We have $\left[\frac{5+i}{7}\right]_4 \equiv (5+i)^{(N(7)-1)/4} = (5+i)^{12} \equiv -i \pmod{7}$ so $\left[\frac{5+i}{7}\right]_4 = \boxed{-i}$. Thus $5+i$ is $\boxed{\text{is not a quadratic or quartic residue}}$ modulo 7.
- Also $\left[\frac{2i}{6+i}\right]_4 \equiv (2i)^{(N(6+i)-1)/4} = (2i)^9 \equiv -1 \pmod{6+i}$ so $\left[\frac{2i}{6+i}\right]_4 = \boxed{-1}$. Therefore, this means that $2i$ $\boxed{\text{is a quadratic residue but not a quartic residue}}$ modulo $6+i$.
- Finally $\left[\frac{-2+i}{7-2i}\right]_4 \equiv (-2+i)^{(N(7-2i)-1)/4} = (-2+i)^{13} \equiv 1 \pmod{7-2i}$ so $\left[\frac{-2+i}{7-2i}\right]_4 = \boxed{1}$. Thus $-2+i$ $\boxed{\text{is a quartic (hence also a quadratic) residue}}$ modulo $7-2i$.

(d) Find the primary associates of the primes 11 and $7+2i$ in $\mathbb{Z}[i]$, and then verify quartic reciprocity for these associates.

- We have $-11 \equiv 1 \pmod{2+2i}$ and also $7+2i \equiv 1 \pmod{2+2i}$, so the desired associates are $\boxed{-11}$ and $\boxed{7+2i}$.
- We have $\left[\frac{-11}{7+2i}\right]_4 \equiv (-11)^{(N(7+2i)-1)/4} = (-11)^{13} \equiv 1 \pmod{7+2i}$ so $\left[\frac{-11}{7+2i}\right]_4 = 1$.
- Also $\left[\frac{7+2i}{11}\right]_4 \equiv (7+2i)^{(N(11)-1)/4} = (7+2i)^{30} \equiv 1 \pmod{11}$ so $\left[\frac{7+2i}{11}\right]_4 = 1$.
- This agrees with quartic reciprocity since $\frac{N(-11)-1}{4} \cdot \frac{N(7+2i)-1}{4}$ is even, so the quartic residue symbols should be equal.

2. Find all solutions (x, y, z) to the Diophantine equation $x^2 + y^2 = z^7$ where x and y are relatively prime.

- Since squares are 0 or 1 modulo 4, one of x, y must be odd and the other is even, and also z is odd.
- Now factor the equation inside the UFD $\mathbb{Z}[i]$ as $(x + iy)(x - iy) = z^5$.
- We now claim that $x + iy$ and $x - iy$ are relatively prime inside $\mathbb{Z}[i]$: this follows the same way as the argument in class for $x^2 + y^2 = z^5$: any common divisor must necessarily divide the sum $2x$ and the difference $2iy$, but since x and y are relatively prime integers, this means that the gcd must divide $2 = -i(1 + i)^2$. Then the only possible Gaussian prime divisor of the gcd is $1 + i$, but $1 + i$ does not divide $x + iy$ because x and y have opposite parity.
- Thus, $x + iy$ and $x - iy$ are relatively prime inside $\mathbb{Z}[i]$. Since their product is a seventh power (namely, z^7) and $\mathbb{Z}[i]$ is a UFD, this means that each term must be a seventh power up to a unit factor.
- But since the only units are $\pm 1, \pm i$ and these are all seventh powers (of their reciprocals), we must have $x + iy = (a + bi)^7 = (a^7 - 21a^5b^2 + 35a^3b^4 - 7ab^6) + (7a^6b - 35a^4b^3 + 21a^2b^5 - b^7)i$. Then the conjugate $x - iy$ is $(a - bi)^7$, and $z^7 = (x + iy)(x - iy) = (a^2 + b^2)^7$.
- Since all such tuples work, the solutions are of the form $(x, y, z) = \boxed{(a^7 - 21a^5b^2 + 35a^3b^4 - 7ab^6,\ 7a^6b - 35a^4b^3 + 21a^2b^5 - b^7,\ a^2 + b^2)}$ for relatively prime integers a and b.

---

3. Prove that the only solution to the Diophantine equation $y^2 = x^3 - 8$ is $(x, y) = (2, 0)$. [Hint: There are two different cases according to whether y is even or odd.]

- If y is even, say with $y = 2p$, then x must also be even, say with $x = 2q$. Then the equation becomes $p^2 = 2q^3 - 2$, so p is even, say $p = 2r$. Then we get $4r^2 = 2q^3 - 2$ so that $2r^2 = q^3 - 1$.
- Rearrange the equation and factor in $\mathbb{Z}[\sqrt{-2}]$ to obtain $q^3 = (1 + r\sqrt{-2})(1 - r\sqrt{-2})$. Since $1 + r\sqrt{-2}$ and $1 - r\sqrt{-2}$ are relatively prime (their sum is 2, and the only irreducible factor $\sqrt{-2}$ of 2 does not divide either term) this means $1 + r\sqrt{-2}$ must be a cube up to a unit factor, hence it actually is a cube.
- Then $1 + r\sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$, so that $a^3 - 6ab^2 = 1$. Factoring yields $a(a^2 - 6b^2) = 1$ and so $a = \pm 1$. The only possibility that yields a valid b is $a = 1$ with $b = 0$, which gives $r = 0$ hence $y = 0$ and $x = 2$. Thus we get the solution $(2, 0)$ in this case.
- Otherwise, if y is odd, rearrange the equation and factor in $\mathbb{Z}[\sqrt{-2}]$ to obtain $x^3 = (y + 2\sqrt{-2})(y - 2\sqrt{-2})$. Then $y + 2\sqrt{-2}$ and $y - 2\sqrt{-2}$ are relatively prime since their difference is $4\sqrt{-2}$ and the only irreducible factor $\sqrt{-2}$ of $4\sqrt{-2}$ does not divide either term since y is odd.
- This means $y + 2\sqrt{-2}$ must be a cube up to a unit factor, hence it actually is a cube.
- Then $y + 2\sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$ so that $3a^2b - 2b^3 = 2$. Factoring yields $b(3a^2 - 2b^2) = 2$ and so b divides 2. But $b = -2$ gives $a^2 = 7/3$, $b = -1$ gives $a = 0$, $b = 1$ gives $a^2 = 4/3$, and $b = 2$ gives $a^2 = 3$, so the only solution comes from $a = 0$, $b = -1$, but this yields $y = 0$ which does not have y odd.
- Thus we get the unique solution $(x, y) = (2, 0)$ as claimed.

---

4. If R is a (commutative) ring with 1, the characteristic of R is defined to be the smallest positive integer n for which $\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}} = 0$, or 0 if there is no such positive integer n.

(a) Find the characteristics of $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}[i]/(7)$, $\mathbb{Z}[i]/(2 + i)$, and $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$. [Note that $(1, 1)$ is the multiplicative identity in the last ring.]

- The characteristic of $\mathbb{Z}$ is $\boxed{0}$, the characteristic of $\mathbb{R}$ is $\boxed{0}$, the characteristic of $\mathbb{Z}/m\mathbb{Z}$ is $\boxed{m}$, the characteristic of $\mathbb{Z}[i]/(7)$ is $\boxed{7}$, the characteristic of $\mathbb{Z}[i]/(2 + i)$ is $\boxed{5}$ (note that $5 \equiv 0 \bmod 2 + i$ but no smaller integer is), and the characteristic of $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ is $\boxed{12}$, since it is straightforward to see that $12 \cdot (1, 1) = (0, 0)$ but no smaller multiple will suffice.

(b) If R is an integral domain, prove that its characteristic is always either 0 or a prime number.

- If the characteristic is 0 we are done, and the characteristic cannot be 1 (since then $1 = 0$) so suppose the characteristic is $n > 1$.
- If $n = ab$ for positive integers a and b, then we have $0 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}} = (\underbrace{1 + 1 + \cdots + 1}_{a \text{ terms}})(\underbrace{1 + 1 + \cdots + 1}_{b \text{ terms}})$.
- But since R is an integral domain, it has no zero divisors, so one of the terms on the right must be zero. By minimality of n, we conclude that either $a = n$ or $b = n$, meaning that n has no nontrivial factorization hence must be prime.

(c) Let R be a commutative ring of prime characteristic p. Prove that for any $a, b \in R$, the "freshman's binomial theorem" $(a + b)^p = a^p + b^p$ is actually correct. Deduce that the map $\varphi : R \to R$ given by $\varphi(a) = a^p$ is actually a ring homomorphism (this map is called the Frobenius endomorphism and turns out to be quite important in many contexts).

- From the (correct) binomial theorem, we know that $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$, so it is sufficient to prove that each of the binomial coefficients $\binom{p}{k}$ for $1 \leq k \leq p-1$ is divisible by p, since by the assumption on the characteristic we know that $p = 0$ in R.
- For this, observe that $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$, and notice that the numerator is divisible by p but the denominator is not (since there is a factor of p in $p!$ but not in any smaller factorial). Thus, the integer quotient is divisible by p, as claimed.
- Finally, we see $\varphi(a+b) = (a+p)^p = a^p + b^p = \varphi(a) + \varphi(b)$ and also $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$ so φ is a ring homomorphism as claimed.

(d) Let p be an integer prime congruent to 3 modulo 4. If $z = a + bi \in \mathbb{Z}[i]$, prove that $z^p \equiv \overline{z} \pmod{p}$. [Note that this was mentioned but not proven in class.]

- Since p is an odd prime, $\mathbb{Z}[i]/(p)$ has characteristic p, as suggested in part (a).
- Then by (c), we have $z^p = (a + bi)^p \equiv a^p + (bi)^p \pmod{p}$.
- By Fermat's little theorem we know that $a^p \equiv a$ and $b^p \equiv b \pmod{p}$, and also since $p \equiv 3 \pmod{4}$ we have $i^p = -i$.
- Putting all of this together yields $z^p = (a + bi)^p \equiv a^p + (bi)^p \equiv a - bi \equiv \overline{z} \pmod{p}$, as claimed.

---

5. Suppose I is a nonzero ideal of $R = \mathcal{O}_{\sqrt{D}}$. The goal of this problem is to show that R/I is finite and its cardinality is $N(I)$. (Indeed, $N(I)$ is often just defined to be the cardinality of R/I, rather than as the nonnegative generator of $I \cdot \overline{I}$.)

(a) Suppose I has prime ideal factorization $I = P_1^{a_1} \cdots P_n^{a_n}$. Show that R/I is isomorphic to $(R/P_1^{a_1}) \times \cdots \times (R/P_n^{a_n})$ and that $N(I) = N(P_1^{a_1}) \cdots N(P_n^{a_n})$.

- First, if P and Q are distinct nonzero prime ideals, then P^a and Q^b are comaximal: any ideal containing both necesssarily divides both, but by the uniqueness of prime ideal factorizations, the only such ideal is $(1) = R$.
- Thus $P_1^{a_1}$, $P_2^{a_2}$, ... , $P_n^{a_n}$ are pairwise comaximal , so the Chinese remainder theorem immediately gives that R/I is isomorphic to $(R/P_1^{a_1}) \times \cdots \times (R/P_n^{a_n})$.
- Finally, we have $N(I) = N(P_1^{a_1}) \cdots N(P_n^{a_n})$ because the norm of ideals is multiplicative.

(b) Suppose a is any positive integer. Show that the cardinality of $R/(a)$ is a^2.

- Observe that $(a) = \{ap + aq\alpha : p, q \in \mathbb{Z}\}$ where α is the generator of $\mathcal{O}_{\sqrt{D}}$.
- Then the elements of $R/(a)$ are uniquely represented as residue classes $p' + q'\alpha$ where $0 \leq p' \leq a-1$ and $0 \leq q' \leq a-1$, and there are $a \cdot a = a^2$ of these.

(c) Suppose $Q = P^n$ is a power of a prime ideal. If $P = (p)$ for a prime integer p, show that $\#(R/Q) = N(Q)$.

- We have $Q = (p)^n = (p^n)$ and also $N(Q) = (p^n)\overline{(p^n)} = p^{2n}$.
- So by (b) we have $\#(R/Q) = (p^n)^2 = p^{2n} = N(Q)$ as claimed.

(d) Suppose $Q = P^n$ for some prime ideal P with $P\overline{P} = (p)$ and p prime; note that we are *not* assuming that $\overline{P} \neq P$. Show that all of the quotients R/P, P/P^2, ... , P^{n-1}/P^n, $P^n/(P^n\overline{P})$, ... , $(P^n\overline{P}^{n-1})/(P^n\overline{P}^n)$ have cardinality greater than 1, and that the product of their cardinalities is the cardinality of $R/(P^n\overline{P}^n)$. Conclude that all of these cardinalities must equal p and deduce that $\#(R/Q) = N(Q)$.

- First, the ideals R, P, P^2, ... , P^{n-1}, P^n, $P^n\overline{P}$, ... , $P^n\overline{P}^{n-1}$, $P^n\overline{P}^n$ must all be distinct by the uniqueness of prime ideal factorizations, since both P and $\overline{P}$ are prime ideals and each factorization has a different number of terms. Therefore, all of the quotients R/P, P/P^2, ... , P^{n-1}/P^n, $P^n/(P^n\overline{P})$, ... , $(P^n\overline{P}^{n-1})/(P^n\overline{P}^n)$ have cardinality greater than 1.
- For the product of the cardinalities we simply apply the following fact about cosets: in any group with subgroups $H_2 \leq H_1$ we have $[G : H_2] = [G : H_1] \cdot [H_1 : H_2]$, which follows simply by noting that each coset of H_1 splits into $[H_1 : H_2]$ cosets of H_2. (One can also deduce this fact from the third isomorphism theorem $R/J \cong (R/I)/(J/I)$ whenever J contains I.)
- Applying this fact repeatedly shows that $\#(R/P)\cdot\#(P/P^2)\cdot\cdots\cdot\#((P^n\overline{P}^{n-1})/(P^n\overline{P}^n)) = \#(R/(P^n\overline{P}^n)) = \#(R/(p^n))$.
- But by (b), $\#(R/(p^n)) = p^{2n}$, and so each of the $2n$ cardinalities of the quotients must be a power of p. But since none of them can equal 1, the only way the product can equal p^{2n} is if all of them are p (otherwise the product would be too large).
- Then by our coset fact again, we have $\#(R/Q) = \#(R/P) \cdot \#(P/P^2) \cdot \cdots \cdot \#(P^{n-1}/P^n) = p^n = N(P)^n = N(Q)$.

(e) Show that R/I has cardinality $N(I)$ for any nonzero ideal I.

- By (a), R/I is isomorphic to $(R/P_1^{a_1}) \times \cdots \times (R/P_n^{a_n})$ and $N(I) = N(P_1^{a_1}) \cdots N(P_n^{a_n})$. Then (c) and (d) show $\#(R/P_i^{a_i}) = N(P_i^{a_i})$ for each prime power $P_i^{a_i}$. Taking the product over all i yields $N(I) = \prod_i N(P_i^{a_i}) = \prod_i \#(R/P_i^{a_i}) = \#\left[\prod_i (R/P_i^{a_i})\right] = \#(R/I)$.

---

6. The goal of this problem is to formulate a general dth-power residue symbol in $\mathbb{Z}/p\mathbb{Z}$, for a prime p (indeed, the construction works in any finite field). So let p be a prime.

(a) Suppose $p \equiv 2 \pmod 3$. Show that every residue class is a cube modulo p. [Hint: The map $x \mapsto x^3$ is a homomorphism on the unit group $(\mathbb{Z}/p\mathbb{Z})^\times$: what is its kernel?]

- Per the hint, we observe that the cubing map $\varphi(x) = x^3$ is a homomorphism on the unit group $(\mathbb{Z}/p\mathbb{Z})^\times$, since it is clearly multiplicative. The kernel of this map consists of the elements with $x^3 \equiv 1 \pmod p$, which is to say, the elements of order dividing 3.
- But since the unit group has order $p - 1 \equiv 1 \pmod 3$, we see that there are no elements of order 3 in this group, so the only element of order dividing 3 is the identity.
- Hence the kernel of φ is trivial, so by the first isomorphism theorem (for groups) we see that the image of φ has cardinality $p - 1$, and so φ is onto: this means every residue class is a cube, as claimed.

(b) Suppose $p \equiv 3 \pmod 4$. Show that every square modulo p is a fourth power modulo p. [Hint: Consider the squaring map on the group of nonzero squares, which has order $(p - 1)/2$.]

- Per the hint, we observe that the squaring map $\varphi(x) = x^2$ is a homomorphism on the group of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$, which has order $(p - 1)/2$. The kernel of this map consists of the elements of order dividing 2.
- But since this group has order $(p - 1)/2 \equiv 1 \pmod 2$, we see that there are no elements of order 2 in this group, so the only element of order dividing 2 is the identity.
- Hence the kernel of φ is trivial, so just as in part (a) that means φ is onto, so that every square residue class is the square of another square, which is to say, a fourth power.

We can see from (a) and (b) that for cubes the only interesting case is when $p \equiv 1 \pmod 3$ and for fourth powers the only interesting case is when $p \equiv 1 \pmod 4$. So we now study the more general situation of dth powers when $p \equiv 1 \pmod d$. So let $d \geq 2$ and let $p \equiv 1 \pmod d$.

(c) Let u be a primitive root modulo p. Show that the dth powers modulo p are $u^d, u^{2d}, \ldots$, and $u^{p-1} = 1$, and also that there are d solutions to $x^d \equiv 1 \pmod p$, given by $u^{(p-1)/d}$, $u^{2(p-1)/d}$, ... , $u^{d(p-1)/d} = 1$.

- Since u is a primitive root, the units are u^1, u^2, ... , $u^{p-1} = 1$ and so the dth powers are u^d, u^{2d}, ... , $u^{d(p-1)/d} = 1$, and after this the powers begin repeating again.

- For the second part, we can see that each of the given elements $u^{(p-1)/d}$, $u^{2(p-1)/d}$, ... , $u^{d(p-1)/d} = 1$ are clearly solutions to $x^d \equiv 1 \pmod{p}$ by Euler's theorem. But they are all distinct and there are d of them, so since the polynomial $x^d - 1$ has at most d roots by unique factorization in $\mathbb{F}_p[x]$, they are all of the roots.

Now define the dth-power residue symbol $\left(\frac{a}{p}\right)_d$ to be the residue class of $a^{(p-1)/d} \pmod{p}$.

(d) Show that $\left(\frac{a}{p}\right)_d = 0$ only when p divides a, and otherwise $\left(\frac{a}{p}\right)_d$ is one of the d solutions to $x^d \equiv 1 \pmod{p}$.

- Obviously $a^{(p-1)/d} \equiv 0$ only when $a \equiv 0 \pmod{p}$. Otherwise, we see that $[a^{(p-1)/d}]^d = a^{p-1} \equiv 1 \pmod{p}$ by Euler's theorem, and so $\left(\frac{a}{p}\right)_d$ is one of the d solutions to $x^d \equiv 1 \pmod{p}$.

(e) Show that $\left(\frac{ab}{p}\right)_d = \left(\frac{a}{p}\right)_d \left(\frac{b}{p}\right)_d$.

- We have $\left(\frac{ab}{p}\right)_d = (ab)^{(p-1)/d} = a^{(p-1)/d} b^{(p-1)/d} = \left(\frac{a}{p}\right)_d \left(\frac{b}{p}\right)_d$ as residue classes modulo p.

(f) Let u be a primitive root modulo p. Show that $\left(\frac{u}{p}\right)_d$ is a primitive dth root of unity modulo p (i.e., its order modulo p is exactly d).

- Suppose the order of $\left(\frac{u}{p}\right)_d$ equals k; then $k \leq d$ by part (d).
- By definition we would have $u^{k(p-1)/d} = 1 \pmod{p}$, so by properties of order this means the exponent $k(p-1)/d$ must be a multiple of the order of u, which is $p-1$.
- This means k/d is an integer and thus that $k \geq d$, so we must have $k = d$.

(g) Show that $\left(\frac{a}{p}\right)_d = 1$ if and only if a is a nonzero dth power modulo p.

- Let u be a primitive root modulo p. If $a = b^d$ for a nonzero b, then $\left(\frac{a}{p}\right)_d = \left(\frac{b}{p}\right)_d^d = 1$ by multiplicativity from (e) and the fact that $\left(\frac{b}{p}\right)_d$ is a dth root of unity by (d).
- Conversely, suppose $\left(\frac{a}{p}\right)_d = 1$ and $a = u^k$. Then $1 = \left(\frac{a}{p}\right)_d = \left(\frac{u}{p}\right)_d^k$ and so since $\left(\frac{u}{p}\right)_d$ is a primitive dth root of unity, this means k is divisible by d, and so $a = (u^{k/d})^d$ is a dth power, as desired.

Remark: As is, we cannot formulate any sort of dth-power reciprocity law, since we cannot compare the dth roots of unity modulo different primes in any sensible way except in the case where $d = 2$. Unfortunately, there is no easy way to fix this problem, since there is no canonical way to identify the roots of unity modulo p with those in $\mathbb{C}$ (if $d > 2$, taking the conjugate gives an equally valid identification). Ultimately, this is why we must work in $\mathcal{O}_{\sqrt{-3}}$ for cubic residue symbols and in $\mathbb{Z}[i]$ for quartic residue symbols, as these rings do possess the necessary complex roots of unity to allow us to compare residue symbols for different primes.

---

7. [Challenge] In class, we proved cubic and quartic reciprocity using properties of Gauss sums. The goal of this problem is to give a self-contained proof of quadratic reciprocity using Gauss sums. So let p, q be distinct odd integer primes and let $\chi_p(a) = \left(\frac{a}{p}\right)$ be the Legendre symbol modulo p. Recall that the Gauss sum of a multiplicative character χ is defined to be $g_a(\chi) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p} \in \mathbb{C}$.

(a) Show that $g_a(\chi_p) = \left(\frac{a}{p}\right) g_1(\chi_p)$ for any integer a. [Hint: If $p|a$, count the number of quadratic residues. For other a, reindex the sum.]

- If $p|a$ then $g_a(\chi_p) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right)$. This sum is zero because there are $(p-1)/2$ quadratic residues, where the Legendre symbol is $+1$, and $(p-1)/2$ quadratic nonresidues, where the Legendre symbol is -1.
- Otherwise if p does not divide a, by changing variables $s = at$ and noting that s also runs over all nonzero residue classes modulo p, we have $g_a(\chi) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) e^{2\pi i a t/p} = \sum_{s=1}^{p-1} \left(\frac{s/a}{p}\right) e^{2\pi i s/p} = \left(\frac{a}{p}\right)^{-1} \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) e^{2\pi i s/p} = \left(\frac{a}{p}\right) g_1(\chi_p)$ since $\left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$.

(b) Let $S = \sum_{a=0}^{p-1} g_a(\chi_p) g_{-a}(\chi_p)$. Show that $S = \left(\frac{-1}{p}\right)(p-1) g_1(\chi)^2$. [Hint: Use (a), making sure to separate $a = 0$ and $a \neq 0$.]

- By (a) we can write $S = \sum_{a=0}^{p-1} g_a(\chi_p) g_{-a}(\chi_p) = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) g_1(\chi) \cdot \left(\frac{-a}{p}\right) g_1(\chi) = \sum_{a=0}^{p-1} \left(\frac{-a^2}{p}\right) g_1(\chi)^2$.
- Since $\left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right)$ for any $a \neq 0$, the given sum is simply $\left(\frac{-1}{p}\right)(p-1) g_1(\chi)^2$, as claimed.

(c) Show that $\sum_{a=0}^{p-1} e^{2\pi i a(s-t)/p} = \begin{cases} p & \text{if } s \equiv t \pmod p \\ 0 & \text{if } s \not\equiv t \pmod p \end{cases}$ for any integers s and t.

- If $s = t$ then the sum is just $\sum_{a=0}^{p-1} 1 = p$.
- Otherwise, if $s \neq t$, the sum is a geometric series and is $\frac{1 - [e^{2\pi i(s-t)/p}]^p}{1 - e^{2\pi i(s-t)/p}} = \frac{1 - e^{2\pi i(s-t)}}{1 - e^{2\pi i(s-t)/p}} = 0$ since $e^{2\pi i a(s-t)} = 1$.

(d) Show that the sum S from part (b) is equal to $p(p-1)$. [Hint: Write $S = \sum_{a=0}^{p-1} \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \left(\frac{st}{p}\right) e^{2\pi i a(s-t)/p}$, then change summation order to sum over a first, move the Legendre symbol out, and use (c).]

- We have $g_a(\chi_p) = \sum_{s=1}^{p-1} \chi(t) e^{2\pi i a s/p}$ and $g_{-a}(\chi_p) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p}$ so multiplying these together yields $g_a(\chi_p) g_{-a}(\chi_p) = \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \left(\frac{st}{p}\right) e^{2\pi i a(s-t)/p}$. Now summing over a gives $S = \sum_{a=0}^{p-1} \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \left(\frac{st}{p}\right) e^{2\pi i a(s-t)/p}$.
- Changing the summation order to sum over a first then gives $S = \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \sum_{a=0}^{p-1} \left(\frac{st}{p}\right) e^{2\pi i a(s-t)/p} = \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \left(\frac{st}{p}\right) \sum_{a=0}^{p-1} e^{2\pi i a(s-t)/p}$.
- Now by (c) we see that the inner sum is equal to p when $s = t$ and is 0 when $s \neq t$, so the sum S reduces to $\sum_{s=1}^{p-1} \left(\frac{s^2}{p}\right) p = p(p-1)$ since the Legendre symbol is always 1.

(e) Let $p^* = \left(\frac{-1}{p}\right) p$. Show that the Gauss sum $g_1(\chi_p)$ has $g_1(\chi_p)^2 = p^*$. Deduce that $g_1(\chi_p)$ is an element of the quadratic integer ring $\mathcal{O}_{\sqrt{p^*}}$.

- Comparing the expressions for S from (b) and (d) yields $p(p-1) = \left(\frac{-1}{p}\right)(p-1)g_1(\chi)^2$ and so $g_1(\chi)^2 = \left(\frac{-1}{p}\right) p = p^*$, as claimed.
- The second statement follows by taking the square root to see $g_1(\chi_p) = \pm\sqrt{p^*} \in \mathcal{O}_{\sqrt{p^*}}$.

Now let p and q be distinct odd primes and let $g = g_1(\chi_p) \in \mathcal{O}_{\sqrt{p^*}}$ be the quadratic Gauss sum.

(f) Show that $g^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. [Hint: Use (e).]

- Since $q-1$ is even, we have $g^{q-1} = (g^2)^{(q-1)/2} = (p^*)^{(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$ by Euler's criterion.

(g) Show that $g^q \equiv g_q(\chi_p) \equiv \left(\frac{q}{p}\right) g \pmod{q}$. [Hint: Use 5(c) and part (a).]

- Using the freshman's binomial theorem mod q, we have $g^q = \left[\sum_{t=1}^{p-1} \chi_p(t) e^{2\pi i t/p}\right]^q \equiv \sum_{t=1}^{p-1} \chi_p(t)^q e^{2\pi i q t/p} = \sum_{t=1}^{p-1} \chi_p(t) e^{2\pi i q t/p} = g_q(\chi_p) \pmod{q}$, where in the middle we used $\chi_p(t)^q = \chi_p(t)$ since q is odd.
- Then (a) gives $g_q(\chi_p) = \left(\frac{q}{p}\right) g$, so we get $g^q \equiv g_q(\chi_p) \equiv \left(\frac{q}{p}\right) g \pmod{q}$ as claimed.

(h) Conclude that $\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q}$, and deduce that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.

- Comparing the expressions from (f) and (g) yields $\left(\frac{q}{p}\right) g \equiv g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q}$. Then multiplying by g and using $g^2 = p^*$ from (e) yields $\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod{q}$, so cancelling p^*, which is invertible mod q, gives $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$.
- Finally, since q is odd and these Legendre symbols are both ± 1, they must actually be equal.

(i) Deduce the law of quadratic reciprocity: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$.

- By Euler's criterion applied to the element $\left(\frac{-1}{p}\right)$ mod q and the fact that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, we have $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{\left(\frac{-1}{p}\right) p}{q}\right) = \left(\frac{\left(\frac{-1}{p}\right)}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{-1}{p}\right)^{(q-1)/2} = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$ as required.
