(*February 24, 2024*)

Proto-Quadratic-Reciprocity

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

---

1. *When is -1 a square mod p?*

For p prime, $(\mathbb{Z}/p)^\times$ is *cyclic* of order $p-1$. A square root of -1 would be of order 4 in that group. By Lagrange's theorem, it is *necessary* that $p = 1 \bmod 4$ for this to be possible. The cyclicness shows that $p = 1 \bmod 4$ is also *sufficient*.

---

2. *Euler's criterion for squares mod p*

Again, for p prime, $(\mathbb{Z}/p)^\times$ is *cyclic* of order $p-1$. Thus, for odd p, non-zero $a \in \mathbb{Z}/p$ is a square if and only if $a^{\frac{p-1}{2}} = 1 \bmod p$.

The *quadratic symbol* of a mod p is

$$\left(\frac{a}{p}\right)_2 \;=\; \begin{cases} 0 & \text{for } a = 0 \bmod p \\ 1 & \text{for } a \text{ a non-zero square mod } p \\ -1 & \text{for } a \text{ a non-zero non-square mod } p \end{cases}$$

Thus,

$$\left(\frac{a}{p}\right)_2 \;=\; a^{\frac{p-1}{2}} \bmod p$$

The large exponent might seem to make this criterion useless in computations. However, using the square-and-multiply algorithm for computing powers, the total number of multiplications is only of the order of $\log p$.

---

3. *When is -3 a square mod p?*

It's easy to find $\sqrt{-3}$ appearing in a cyclotomic field: the third cyclotomic polynomial is merely quadratic:

$$\Phi_3(x) \;=\; \frac{x^3-1}{x-1} \;=\; x^2+x+1$$

so

$$\omega \;=\; \frac{-1\pm\sqrt{-3}}{2}$$

Thus,

$$\omega - \omega^{-1} \;=\; \sqrt{-3}$$

Then, on one hand,

$$(\omega-\omega^{-1})^p \;=\; \omega^p + \omega^{-p} \qquad \text{(mod } p\text{... inner binomial coefficients are 0 mod } p\text{)}$$

On the other hand, mod p,

$$(\omega-\omega^{-1})^p \;=\; (\sqrt{-3})^p \;=\; (-3)^{\frac{p-1}{2}}\cdot(\sqrt{-3})$$

and (yes, we can divide mod p)

$$\frac{(\omega-\omega^{-1})^p}{\sqrt{-3}} \;=\; (-3)^{\frac{p-1}{2}} \;=\; \left(\frac{-3}{p}\right)_2 \bmod p$$

Thus, (with $p \neq 3$)

$$\binom{-3}{p}_2 = \frac{\omega^p - \omega^{-p}}{\sqrt{-3}} = \begin{cases} \dfrac{\omega - \omega^{-1}}{\sqrt{-3}} & \text{for } p = 1 \bmod 3 \\ \dfrac{\omega^{-1} - \omega}{\sqrt{-3}} & \text{for } p = -1 \bmod 3 \end{cases} = \begin{cases} 1 & \text{for } p = 1 \bmod 3 \\ -1 & \text{for } p = -1 \bmod 3 \end{cases}$$

From an elementary viewpoint, it is completely surprising that the outcome is periodic in p!

---

4. *When is* 2 *a square mod* p*?*

Of course, a primitive eighth root of unity ω is a zero of the eighth cyclotomic polynomial $\Phi_8(x) = \frac{x^8-1}{x^4-1} = x^4+1$. Anticipating the irreducibility of this polyomial in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, the field extension $\mathbb{Q}(\omega)$ of $\mathbb{Q}$ is of degree 4. Anticipating Galois theory, there should be an intermediate quadratic field. But we do not need to invoke that, because there is an appealing *ad hoc* device, demonstrating that intermediate quadratic field directly.

Namely, $\omega^4 + 1 = 0$ gives $\omega^2 + \omega^{-2} = 0$. The inverse-symmetry of this suggests looking for a lower-degree equation for $\alpha = \omega + \omega^{-1}$. As expected,

$$\alpha^2 = (\omega + \omega^{-1})^2 = \omega^2 + 2 + \omega^{-2} = 0 + 2 = 2$$

With p an odd prime, on one hand,

$$(\omega + \omega^{-1})^p = \omega^p + \sum_{1 \le k \le p-1} \binom{p}{k} \omega^{p-k}\omega^{-k} + \omega^{-p} = \omega^p + \omega^{-p} \qquad (\text{in } \mathbb{Z}[\omega] \bmod p\mathbb{Z}[\omega])$$

On the other hand,

$$(\omega + \omega^{-1})^p = (\sqrt{2})^p = 2^{\frac{p-1}{2}} \cdot \sqrt{2} \qquad (\text{apparently in } \mathbb{Z}[\omega])$$

Thus,

$$\omega^p + \omega^{-p} = 2^{\frac{p-1}{2}} \cdot \sqrt{2} \qquad (\text{in } \mathbb{Z}[\omega])$$

and the same equality certainly holds in $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$. Since $\gcd(2,p) = 1$, $\sqrt{2}$ is invertible in the latter quotient ring, so divide through by $\sqrt{2}$:

$$\binom{2}{p}_2 = 2^{\frac{p-1}{2}} \bmod p = \frac{\omega^p + \omega^{-p}}{\sqrt{2}} \bmod p = \begin{cases} \frac{\omega+\omega^{-1}}{\sqrt{2}} & \text{for } p = 1 \bmod 8 \\ \frac{\omega^3+\omega^{-3}}{\sqrt{2}} & \text{for } p = 3 \bmod 8 \\ \frac{\omega^5+\omega^{-5}}{\sqrt{2}} & \text{for } p = 5 \bmod 8 \\ \frac{\omega^7+\omega^{-7}}{\sqrt{2}} & \text{for } p = 7 \bmod 8 \end{cases}$$

The latter really is the explanatory answer. For specific numerical outcomes, a little computation gives

$$\binom{2}{p}_2 = \begin{cases} 1 & \text{for } p = 1,7 \bmod 8 \\ -1 & \text{for } p = 3,5 \bmod 8 \end{cases}$$

---

5. *When is* 5 *a square mod* p*?*

The appearance of $\sqrt{5}$ in cyclotomic fields is slightly less obvious, from an elementary viewpoint, than $\sqrt{2}$ and $\sqrt{-3}$. Still, it is iconic: a primitive fifth root of unity ω satisfies

$$0 \;=\; \frac{\omega^5-1}{\omega-1} \;=\; \omega^4+\omega^3+\omega^2+\omega+1$$

The standard device to exploit front-to-back symmetry of that polynomial is to divide the latter equation by ω^2, and let $\alpha = \omega+\omega^{-1}$, so

$$0 \;=\; \omega^2+\omega+1+\omega^{-1}+\omega^{-2} \;=\; (\alpha^2-2)+\alpha+1 \;=\; \alpha^2+\alpha-1$$

Then

$$\alpha \;=\; \frac{-1\pm\sqrt{1+4}}{2} \;=\; \frac{-1\pm\sqrt{5}}{2}$$

By the way, taking the choice of sign to give a positive real number, this gives

$$2\cos 70^o \;=\; \frac{\sqrt{5}-1}{2}$$

For purposes of computing $\left(\frac{5}{p}\right)_2$, rearrange the expression for α to $2\alpha+1 = \sqrt{5}$, which is

$$\sqrt{5} \;=\; 2\omega+1+2\omega^{-1}$$

Then, for odd prime $p \neq 5$, mod p,

$$\left(\frac{5}{p}\right)_2 \;=\; 5^{\frac{p-1}{2}} \;=\;=\; (2\omega^2+1+2\omega^{-2})^{p-1} \qquad\qquad (\text{mod } p, \text{ in } \mathbb{Z}[\omega])$$

To be able to use the divisibility-by-p of the inner binomial/multinomial coefficients $\binom{p}{i}$, multiply through by $\sqrt{5}$, a *unit* mod p:

$$\sqrt{5}\left(\frac{5}{p}\right)_2 \;=\; (2\omega+1+2\omega^{-1})^p \;=\; (2\omega)^p+1^p+(2\omega^{-1})^p \qquad\qquad (\text{mod } p, \text{ in } \mathbb{Z}[\omega])$$

By Fermat's Little Theorem, $2^p = 2 \bmod p$, so this is

$$\left(\frac{5}{p}\right)_2 \;=\; \frac{2\omega^p+1+2\omega^{-p}}{\sqrt{5}}$$

Already the qualitative point is clear, that the quadratic symbol is periodic in p mod 5. Numerically,

$$\left(\frac{5}{p}\right)_2 \;=\; \begin{cases} \dfrac{2\omega+1+2\omega^{-1}}{\sqrt{5}} & = & \dfrac{\sqrt{5}}{\sqrt{5}} & = & 1 & \text{for } p = 1 \bmod 5 \\ \dfrac{2\omega^2+1+2\omega^{-2}}{\sqrt{5}} & = & & = & -1 & \text{for } p = 2 \bmod 5 \\ \dfrac{2\omega^3+1+2\omega^{-3}}{\sqrt{5}} & = & \dfrac{2\omega^{-2}+1+2\omega^2}{\sqrt{5}} & = & -1 & \text{for } p = 3 \bmod 5 \\ \dfrac{2\omega^4+1+2\omega^{-4}}{\sqrt{5}} & = & \dfrac{2\omega+1+2\omega^{-1}}{\sqrt{5}} & = & 1 & \text{for } p = 4 \bmod 5 \end{cases}$$