Roots of Unity and Quadratic Reciprocity

Remember our proof that $p \equiv 1 \bmod 4$ if and only if $\left(\frac{-1}{p}\right) = 1$:

Remember our proof that $p \equiv 1 \bmod 4$ if and only if $\left(\frac{-1}{p}\right) = 1$:

Since U_p is cyclic, we have $p \equiv 1 \bmod 4$ if and only if there is a primitive 4-th root of unity, ζ_4, in U_p.

Remember our proof that $p \equiv 1 \bmod 4$ if and only if $\left(\frac{-1}{p}\right) = 1$:

Since U_p is cyclic, we have $p \equiv 1 \bmod 4$ if and only if there is a primitive 4-th root of unity, ζ_4, in U_p.

But ζ_4 is a primitive 4-th root of unity if and only if $\zeta_4^2 = -1$.

Gauss gave a similar proof that, if $p \equiv 1 \bmod 8$, then $\left(\frac{2}{p}\right) = 1$.

Since U_p is cyclic, there is a primitive 8-th root of unity, ζ_8, in U_p.

Gauss gave a similar proof that, if $p \equiv 1 \bmod 8$, then $\left(\frac{2}{p}\right) = 1$.

Since U_p is cyclic, there is a primitive 8-th root of unity, ζ_8, in U_p.

Gauss pulls a rabbit out of his hat! Define

 $= \zeta_8 + \zeta_8^{-1}$.

Gauss gave a similar proof that, if $p \equiv 1 \bmod 8$, then $\left(\frac{2}{p}\right) = 1$.

Since U_p is cyclic, there is a primitive 8-th root of unity, ζ_8, in U_p.

Gauss pulls a rabbit out of his hat! Define

 $= \zeta_8 + \zeta_8^{-1}$.

 $^2 = \left(\zeta_8 + \zeta_8^{-1}\right)^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = 2.$

Here is another example: If $p \equiv 1 \bmod 3$ then $\left(\frac{-3}{p}\right) = 1$:

Since U_p is cyclic, there is a primitive 3-rd root of unity, ζ_3, in U_p. Define:

$$_3 = \zeta_3 - \zeta_3^{-1}$$

Here is another example: If $p \equiv 1 \bmod 3$ then $\left(\frac{-3}{p}\right) = 1$:

Since U_p is cyclic, there is a primitive 3-rd root of unity, ζ_3, in U_p. Define:

$$\text{  }_3 = \zeta_3 - \zeta_3^{-1}$$

Then

$$\left(\text{  }_3\right)^2 = \left(\zeta_3 - \zeta_3^{-1}\right)^2 = \zeta_3^2 - 2 + \zeta_3^{-2} = \zeta_3^2 - 2 + \zeta_3 = -3$$

since $\zeta_3^2 + \zeta_3 + 1 = 0$.

Here is another example: If $p \equiv 1 \bmod 3$ then $\left(\frac{-3}{p}\right) = 1$:

Since U_p is cyclic, there is a primitive 3-rd root of unity, ζ_3, in U_p. Define:


$$_3 = \zeta_3 - \zeta_3^{-1}$$

Then

$$\left(\quad_3\right)^2 = \left(\zeta_3 - \zeta_3^{-1}\right)^2 = \zeta_3^2 - 2 + \zeta_3^{-2} = \zeta_3^2 - 2 + \zeta_3 = -3$$

since $\zeta_3^2 + \zeta_3 + 1 = 0$.

In this case, the argument is reversible: If there is a square root of -3 modulo p, then $\frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.

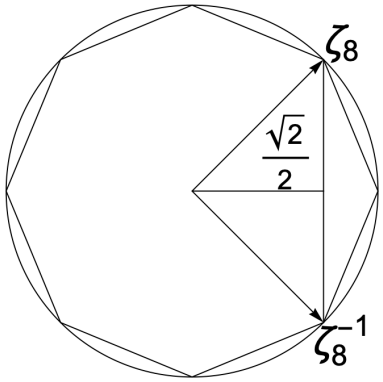
Let's do one more: If $p \equiv 1 \bmod 5$ then $\left(\frac{5}{p}\right) = 1$: Since U_p is cyclic, there is a primitive 5-th root of unity, ζ_5, in U_p. Define:

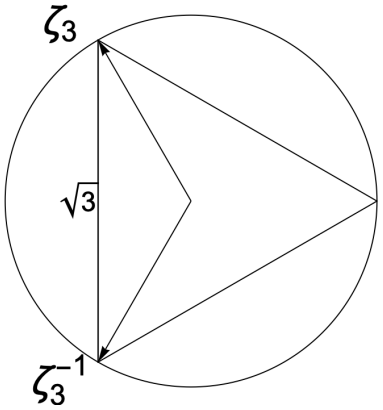
$$\text{  }_5 = \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}.$$

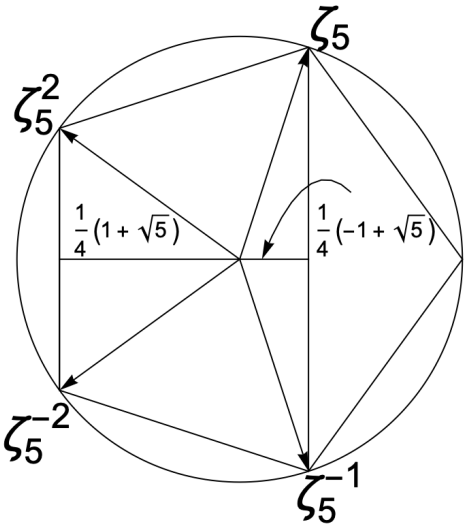
Then

$$\begin{aligned}
\left(\text{  }_5\right)^2 &= \left(\zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}\right)^2 \\
&= \zeta_5^4 - 2\zeta_5^3 + \zeta_5^2 - 2\zeta_5 + 4 - 2\zeta_5^{-1} + \zeta_5^{-2} - 2\zeta_5^{-3} + \zeta_5^{-4} \\
&= -\zeta_5^4 - \zeta_5^3 - \zeta_5^2 - \zeta_5 + 4 = 5.
\end{aligned}$$

These formulas are a little less magic if we look at them geometrically







$$\text{rabbit}_2 = \zeta_8 + \zeta_8^{-1} \qquad \text{rabbit}_3 = \zeta_3 - \zeta_3^{-1} \qquad \text{rabbit}_5 = \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}$$

This suggests a general strategy: Find an element  in $\mathbb{Z}[\zeta_q]$ with $\left(\text{  }\right)^2 = \pm q$. Then we deduce a proof that, if $p \equiv 1 \bmod q$, then $\left(\frac{\pm q}{p}\right) = 1$.

This suggests a general strategy: Find an element  $_q$ in $\mathbb{Z}[\zeta_q]$ with $\left(\right.$  $_q\left.\right)^2 = \pm q$. Then we deduce a proof that, if $p \equiv 1 \bmod q$, then $\left(\frac{\pm q}{p}\right) = 1$.

Notice that we can do the computation $\left(\right.$  $_q\left.\right)^2 = \pm q$ in $\mathbb{C}$, and then deduce that it works in $\mathbb{F}_p$. The minimal polynomial of ζ_q is $x^{q-1} + x^{q-2} + \cdots + x + 1$. If we have some $g(x)$ in $\mathbb{Z}[x]$ with $g(\zeta_q)^2 = \pm q$, then $x^{q-1} + x^{q-2} + \cdots + x + 1$ divides $g(x)^2 \mp q$ in $\mathbb{Z}[x]$, so $x^{q-1} + x^{q-2} + \cdots + x + 1$ also divides $g(x)^2 \mp q$ in $\mathbb{F}_p[x]$.

Lemma: Let q be an odd prime. Then $\sqrt{(-1)^{(q-1)/2}\ q}$ is in $\mathbb{Z}[\zeta_q]$.

Lemma: Let q be an odd prime. Then $\sqrt{(-1)^{(q-1)/2}\, q}$ is in $\mathbb{Z}[\zeta_q]$.

Proof: Define

$$\left(\frac{\cdot}{q}\right) = \prod_{a=1}^{(q-1)/2} \left(\zeta_q^a - \zeta_q^{-a}\right).$$

Then

$$\left(\frac{\cdot}{q}\right)^2 = \prod_{a=1}^{(q-1)/2} \left(\zeta_q^a - \zeta_q^{-a}\right)^2 = \prod_{a=1}^{(q-1)/2} \left(\zeta_q^{2a} - 1\right)\left(1 - \zeta_q^{-2a}\right)$$

$$= (-1)^{(q-1)/2} \prod_{b=1}^{q-1} (1 - \zeta_q^b).$$

Since $\prod_{b=1}^{q-1}(x - \zeta_q^b) = x^{q-1} + x^{q-2} + \cdots + x + 1$, we have
$\prod_{b=1}^{q-1}(1 - \zeta_q^b) = 1 + 1 + \cdots + 1 + 1 = q$. $\square$

There are many other ways to prove this Lemma. For the rest of the talk, it doesn't matter which proof we use, we just need to know that $\sqrt{(-1)^{(q-1)/2}\, q}$ is in $\mathbb{Z}[\zeta_q]$. We'll put $(-1)^{(q-1)/2} q = q^*$.

We now know that, if $p \equiv 1 \bmod q$, then $\left(\frac{q^*}{p}\right) = 1$ where $q^* = (-1)^{(q-1)/2} q$.

We now know that, if $p \equiv 1 \bmod q$, then $\left(\frac{q^*}{p}\right) = 1$ where $q^* = (-1)^{(q-1)/2} q$.

What about other values modulo q?

We now know that, if $p \equiv 1 \bmod q$, then $\left(\frac{q^*}{p}\right) = 1$ where $q^* = (-1)^{(q-1)/2} q$.

What about other values modulo q? Let's start with $\left(\frac{2}{p}\right)$.

Go to a splitting field K of $x^8 - 1$ over $\mathbb{F}_p$. So there is a primitive 8-th root of unity, ζ_8, in K. Set  $= \zeta_8 + \zeta_8^{-1}$. So $($  $)^2 = 2$.

What we need to figure out is whether  is in $\mathbb{F}_p$ or not.

Inside K, we can describe $\mathbb{F}_p$ as the set of solutions to $x^p = x$. So we want to figure out whether or not $\left(\text{  }_2\right)^p = \text{  }_2$:

Inside K, we can describe $\mathbb{F}_p$ as the set of solutions to $x^p = x$. So we want to figure out whether or not $\left(\text{  }_2\right)^p = \text{  }_2$:

$$\left(\text{  }_2\right)^p = \left(\zeta_8 + \zeta_8^{-1}\right)^p \equiv \zeta_8^p + \zeta_8^{-p} \bmod p.$$

Inside K, we can describe $\mathbb{F}_p$ as the set of solutions to $x^p = x$. So we want to figure out whether or not $\left(\text{  }_2\right)^p = \text{  }_2$:

$$\left(\text{  }_2\right)^p = \left(\zeta_8 + \zeta_8^{-1}\right)^p \equiv \zeta_8^p + \zeta_8^{-p} \bmod p$$

$$= \begin{cases} \text{  }_2 & p \equiv \pm 1 \bmod 8 \\ -\text{  }_2 & p \equiv \pm 3 \bmod 8 \end{cases}$$

$$\left(\text{  }_2\right)^p \equiv \begin{cases} \text{  }_2 & p \equiv \pm 1 \bmod 8 \\ -\text{  }_2 & p \equiv \pm 3 \bmod 8 \end{cases} \qquad \bmod p.$$

So $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \bmod 8$.

More generally, I claim that

$$\left(\ \right)^p \equiv \left(\frac{q^*}{p}\right) \ \text{mod } p \text{ in } \mathbb{Z}[\zeta_q].$$

q

q

More generally, I claim that

$$(\ \text{  }\ )^p \equiv \left(\frac{q^*}{p}\right) \text{  } \mod p \text{ in } \mathbb{Z}[\zeta_q].$$

Indeed,

$$(\ \text{  }\ )^p = \left((\ \text{  }\ )^2 \right)^{(p-1)/2} \text{  }$$

$$= (q^*)^{(p-1)/2} \text{  } \equiv \left(\frac{q^*}{p}\right) \text{  } \mod p.$$

Finally, it is time to bring in the Galois theory! We have $\mathrm{Aut}(\mathbb{Q}[\zeta_q]/\mathbb{Q}) = U_q$. For $a \in U_q$, let g_a be the automorphism $\zeta_q \mapsto \zeta_q^a$ of $\mathbb{Q}[\zeta_q]$. So $g_a\left(\sum c_j \zeta_q^j\right) = \sum c_j \zeta_q^{aj}$.

Finally, it is time to bring in the Galois theory! We have $\mathrm{Aut}(\mathbb{Q}[\zeta_q]/\mathbb{Q}) = U_q$. For $a \in U_q$, let g_a be the automorphism $\zeta_q \mapsto \zeta_q^a$ of $\mathbb{Q}[\zeta_q]$. So $g_a\left(\sum c_j \zeta_q^j\right) = \sum c_j \zeta_q^{aj}$.

Notice that, if p is a prime $\neq q$, then, for every $z = \sum c_j \zeta_q^j \in \mathbb{Z}[\zeta_q]$, we have

$$g_p(z) = \sum c_j \zeta_q^{pj} \equiv \left(\sum c_j \zeta_q^j\right)^p = z^p \bmod p.$$

$$g_p\Big(\ \Big)_q \equiv \Big(\ \Big)_q^{\,p} \equiv \left(\frac{q^*}{p}\right)\ \Big)_q \mod p$$

$$g_p\Big(\ \Big)_q \equiv \Big(\ \Big)_q^{\,p} \equiv \left(\frac{q^*}{p}\right)\ \Big)_q \mod p$$

But, since g_p is an automorphism, and $\Big(\ \Big)_q^{\,2}$ is rational, we must have $g_p\Big(\ \Big)_q = \pm\ \Big)_q$. So

$$g_p\Big(\ \Big)_q = \left(\frac{q^*}{p}\right)\ \Big)_q .$$

$$g_p\Big(\ \Big)_q = \left(\frac{q^*}{p}\right)\ \Big)_q .$$

There are many ways we could compute $g_p\Big(\ \Big)_q$. We could do it using our explicit formula for $\ \Big)_q$, or using other explicit formulas for $\ \Big)_q$. But let's do something slicker.

We know that $\left(\frac{\square}{q}\right)^2$ is in $\mathbb{Q}$. So $g \mapsto g\left(\frac{\square}{q}\right)/\frac{\square}{q}$ must be a character from $\mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $\{\pm 1\}$.

We know that $\left(\frac{\text{  }}{q}\right)^2$ is in $\mathbb{Q}$. So $g \mapsto g\left(\frac{\text{  }}{q}\right) / \frac{\text{  }}{q}$ must be a character from $\mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $\{\pm 1\}$.

In other words, $a \mapsto g_a\left(\frac{\text{  }}{q}\right) / \frac{\text{  }}{q}$ must be a character from U_q to $\{\pm 1\}$.

We know that $\left(\frac{\square}{q}\right)^2$ is in $\mathbb{Q}$. So $g \mapsto g\left(\frac{\square}{q}\right) / \frac{\square}{q}$ must be a character from $\mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $\{\pm 1\}$.

In other words, $a \mapsto g_a\left(\frac{\square}{q}\right) / \frac{\square}{q}$ must be a character from U_q to $\{\pm 1\}$.

But U_q is a cyclic group! There is only one nontrivial character from U_q to $\{\pm 1\}$.

We know that $\left(\frac{\ }{q}\right)^2$ is in $\mathbb{Q}$. So $g \mapsto g(\frac{\ }{q})/\frac{\ }{q}$ must be a character from $\mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $\{\pm 1\}$.

In other words, $a \mapsto g_a(\frac{\ }{q})/\frac{\ }{q}$ must be a character form U_q to $\{\pm 1\}$.

But U_q is a cyclic group! There is only one nontrivial character from U_q to $\{\pm 1\}$.

That character is $a \mapsto \left(\frac{a}{q}\right)$.

We know that $\left(\frac{\square}{q}\right)^2$ is in $\mathbb{Q}$. So $g \mapsto g(\frac{\square}{q})/\frac{\square}{q}$ must be a character from $\mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $\{\pm 1\}$.

In other words, $a \mapsto g_a(\frac{\square}{q})/\frac{\square}{q}$ must be a character from U_q to $\{\pm 1\}$.

But U_q is a cyclic group! There is only one nontrivial character from U_q to $\{\pm 1\}$.

That character is $a \mapsto \left(\frac{a}{q}\right)$.

So we deduce

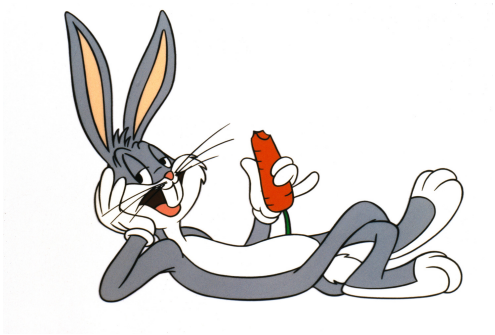
$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

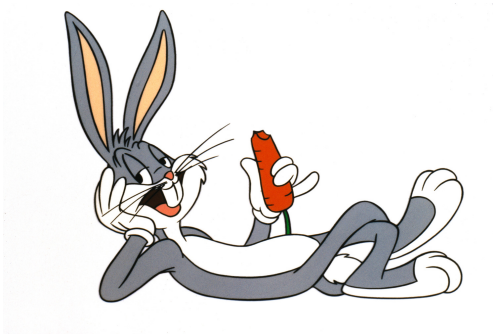
$$\left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{(q-1)/2}q}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2*(q-1)/2}\left(\frac{q}{p}\right)$$

So

$$(-1)^{(p-1)/2*(q-1)/2}\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)!$$



That's all folks!!!!!



That's just the beginning, folks!!!!!

$$\sqrt{17} = \begin{array}{c} \zeta_{17} + \zeta_{17}^2 - \zeta_{17}^3 + \zeta_{17}^4 - \zeta_{17}^5 - \zeta_{17}^6 - \\ \zeta_{17}^7 + \zeta_{17}^8 + \zeta_{17}^9 - \zeta_{17}^{10} - \zeta_{17}^{11} - \zeta_{17}^{12} + \\ \zeta_{17}^{13} - \zeta_{17}^{14} + \zeta_{17}^{15} + \zeta_{17}^{16} \end{array}$$

What if we used a character $U_q \to \{1, \omega, \omega^2\}$ instead?

So many more questions . . . Thank you for taking my class!