MATH 565: Week 13 Notes

Steven C. White

November 30, 2019

How Do We Solve $\left(\frac{2}{p}\right)$?

$$\begin{aligned}
\left(\frac{2}{p}\right) &= \left(\frac{-(-2)}{p}\right) \\
&= \left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right) \\
&= \left(\frac{-1}{p}\right)\left(\frac{p-2}{p}\right) \\
&= \left(\frac{-1}{p}\right)\left(\frac{p}{p-2}\right) \quad \text{p and p-2 cannot both be} \equiv 3 (\text{mod } 4) \\
&= \left(\frac{-1}{p}\right)\left(\frac{2}{p-2}\right) \quad \text{repeat this process} \\
&= \left(\frac{-1}{p}\right)\left(\frac{-1}{p-2}\right)\cdots\left(\frac{-1}{3}\right) \\
&= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-3}{2}}\cdots(-1)^{2}(-1)^{1} \\
&= (-1)^{1+2+\cdots+\frac{p-3}{2}+\frac{p-1}{2}} \\
&= (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)} \\
&= (-1)^{\frac{p^2-1}{8}}
\end{aligned}$$

Then,

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p^2 \equiv 1 \text{ (mod 16)} \Leftrightarrow p \equiv 1,7 \text{ (mod 8)} \\ -1 & \text{if } p^2 \equiv 1 \text{ (mod 8)} \Leftrightarrow p \equiv 3,5 \text{ (mod 8)} \end{cases}$$

Frequency Patterns of QR's (see table at the end of the document). So for any odd prime it seems that there might be $\frac{p-1}{2}$ number of QRs and nQRs. Are there any patterns to the table? How often are two quadratic residues next to eachother? For p=29, there are 6 n where $\left(\frac{n}{29}\right) = \left(\frac{n+1}{29}\right) = 1$. If quadratic residues are "random" like coin flips we would expect around $\frac{p-1}{4}$ of the residues to be consecutive QRs.
Theorem 1: For any fixed a and b and prime p

$$\sum_{n=0}^{p-1}\left(\frac{(n-a)(n-b)}{p}\right) = \begin{cases} p-1 & \text{if } a \equiv b \text{ (mod p)} \\ -1 & \text{otherwise} \end{cases}$$

Proof. Consider the sum over a complete residue class (mod p)

$$\sum_{n(modp)}\left(\frac{(n-a)(n-b)}{p}\right)$$

As n ranges through all residues (mod p), so does (n-a) so we can shift the index (n-a) $\to$ n.

$$\sum_{n(modp)}\left(\frac{n(n-b+a)}{p}\right)$$

If $a \equiv b$ (mod p), then $a - b \equiv 0$ (mod p). So the sum becomes

$$\sum_{n(modp)}\left(\frac{n^2}{p}\right) = p-1$$

Now let $a \not\equiv b$ (mod p), and let $\lambda \equiv a - b$ (mod p). So our sum becomes

$$\sum_{n(modp)}\left(\frac{n(n+\lambda)}{p}\right) = \sum_{\substack{n(modp)\\ n\not\equiv 0(modp)}}\left(\frac{n(n+\lambda)}{p}\right)$$

If $n \not\equiv 0$ (mod p), then n^{-1} exists and $\left(\frac{(n^{-1})^2}{p}\right) = 1$. So we can write

$$\sum_{\substack{n (mod p)\\ n \not\equiv 0 (mod p)}} \left(\frac{n(n+\lambda)}{p}\right) = \sum_{\substack{n (mod p)\\ n \not\equiv 0 (mod p)}} \left(\frac{(n^{-1})^2}{p}\right)\left(\frac{n(n+\lambda)}{p}\right) = \sum_{\substack{n (mod p)\\ n \not\equiv 0 (mod p)}} \frac{1+\lambda n^{-1}}{p}$$

As n varies over a complete nonzero residue class, so does n^{-1} (mod p). So we can write the sum as

$$\sum_{\substack{m (mod p)\\ m \not\equiv 0 (mod p)}} \frac{1+\lambda m}{p}$$

As m varies over a complete nonzero residue class, so does λm (mod p). So we can write the sum as

$$\sum_{\substack{l (mod p)\\ l \not\equiv 0 (mod p)}} \left(\frac{1+l}{p}\right) = \sum_{l=1}^{p-1} \left(\frac{1+l}{p}\right) = \sum_{l=2}^{p} \left(\frac{l}{p}\right) = 0 - \left(\frac{1}{p}\right) = -1$$

Theorem 2: Let p be an odd prime. Let N(p) be the number of consecutive QRs (mod p). Then,

$$N(p) = \frac{1}{4}(p - 4 - (-1)^{\frac{p-1}{2}})$$

Proof. First note that

$$\sum_{n=1}^{p-2} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \sum_{n=0}^{p-1} \left(\frac{n(n+1)}{p}\right) = -1 \text{ by Theorem 1}$$

Let

$$C_p(n) := \frac{1}{4}\left(1 + \left(\frac{n}{p}\right)\right)\left(1 + \left(\frac{n+1}{p}\right)\right) = \begin{cases} 1 & \text{if n and n+1 are both QR} \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\begin{aligned}
N(p) &= \sum_{n=1}^{p-2} C_p(n) \\
&= \sum_{n=1}^{p-2} \frac{1}{4}\left(1 + \left(\frac{n}{p}\right)\right)\left(1 + \left(\frac{n+1}{p}\right)\right) \\
&= \frac{1}{4}\sum_{n=1}^{p-2} 1 + \left(\frac{n}{p}\right) + \left(\frac{n+1}{p}\right) + \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) \\
&= \frac{1}{4}\left(\sum_{n=1}^{p-2} 1 + \sum_{n=1}^{p-2}\left(\frac{n}{p}\right) + \sum_{n=1}^{p-2}\left(\frac{n+1}{p}\right) + \sum_{n=1}^{p-2}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\right) \\
&= \frac{1}{4}\left(p - 2 - \left(\frac{p-1}{p}\right) - \left(\frac{1}{p}\right) - 1\right) \\
&= \frac{1}{4}\left(p - 4 - \left(\frac{-1}{p}\right)\right) \\
&= \frac{1}{4}\left(p - 4 - (-1)^{\frac{p-1}{2}}\right)
\end{aligned}$$

n	$\left(\frac{n}{29}\right)$
1	1
2	-1
3	-1
4	1
5	1
6	1
7	1
8	-1
9	1
10	-1
11	-1
12	-1
13	1
14	-1
15	-1
16	1
17	-1
18	-1
19	-1
20	1
21	-1
22	1
23	1
24	1
25	1
26	-1
27	-1
28	1
29	0