Math 445 Homework 6 Solutions

26. If p is an odd prime and a is a primitive root mod p, then $\left(\frac{a}{p}\right) = -1$.

By Euler's criterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Since a is a primitive root mod p, $\mathrm{ord}_p(a) = p-1$, so $x = a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, since $\frac{p-1}{2} < p-1$. but $x^2 = a^{p-1} \equiv 1 \pmod{p}$ so, since p is prime, $a \equiv \pm 1 \pmod{p}$. So $x \equiv -1$, so $-1 \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$, So $\left(\frac{a}{p}\right) = -1$.

27. The Fermat number $F_n = 2^{2^n} + 1$, for $n \geq 1$, is prime $\Leftrightarrow 3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

($\Rightarrow$:) If F_n is prime, then $3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$. But by quadratic reciprocity, $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)(-1)^{\frac{F_n-1}{2}\frac{3-1}{2}} = \left(\frac{F_n}{3}\right)(-1)^{2^{2^2-1}} = \left(\frac{F_n}{3}\right) = \left(\frac{2^{2^n}+1}{3}\right) = \left(\frac{(-1)^{2^n}+1}{3}\right) = \left(\frac{1+1}{3}\right) = \left(\frac{2}{3}\right) \equiv 2^{\frac{3-1}{2}} = 2^1 = 2 \equiv -1 \pmod{3}$, so $Big(\frac{3}{F_n}\Big) = -1$. So $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

($\Leftarrow$:) If $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ then since $F_n - 1 = 2^{2^n}$ is a power of 2, for every prime $p | F_n - 1$, we have found an a with $a^{\frac{F_n-1}{p}} \equiv -1 \pmod{F_n}$, so by Lucas' Theorem, F_n is prime.

28. The primes p for which $x^2 \equiv 13 \pmod{p}$ has solutions:

Every integer n is congruent to one of $-6, -5, \ldots, 5, 6$ mod 13. By quadratic reciprocity, $\left(\frac{13}{p}\right)\left(\frac{p}{13}\right) = (-1)^{\frac{13-1}{2}\frac{p-1}{2}} = (-1)^{6\cdot\frac{p-1}{2}} = 1$, so $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$. Since we can, in this calculation, work with the residue of p mod 13, rather than with p, it suffices to compute these Legendre symbols for $n = -6$ through $n = 6$. Each of these numbers is a product of the numbers $-1, 2, 3$, and 5, so it suffices to compute Legendre symbols for them.

$\left(\frac{-1}{13}\right) = (-1)^{\frac{13-1}{2}} = (-1)^6 = 1$. $\qquad \left(\frac{2}{13}\right) = (-1)\frac{13^2-1}{8} = (-1)^{21} = -1$.

$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right)(-1)^{\frac{13-1}{2}\frac{3-1}{2}} = \left(\frac{13}{3}\right)(-1)^6 = \left(\frac{13}{3}\right) = \left(\frac{12+1}{3}\right)\left(\frac{1}{3}\right) = 1^6 = 1$. And

$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right)(-1)^{\frac{13-1}{2}\frac{5-1}{2}} = \left(\frac{13}{5}\right)(-1)^{12} = \left(\frac{13}{5}\right) = \left(\frac{10+3}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)(-1)^{\frac{5-1}{2}\frac{3-1}{2}} = \left(\frac{5}{3}\right)(-1)^2 = \left(\frac{5}{3}\right) = \left(\frac{3+2}{3}\right) = \left(\frac{2}{3}\right) = (-1)\frac{3^2-1}{8} = (-1)^1 = -1$. So:

$\left(\frac{-1}{13}\right) = 1, \left(\frac{2}{13}\right) = -1, \left(\frac{3}{13}\right) = 1$ and $\left(\frac{5}{13}\right) = -1$. So:

$\left(\frac{-6}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (1)(-1)(1) = -1 \qquad \left(\frac{-5}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{5}{13}\right) = (1)(-1) = -1$

$\left(\frac{-4}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = (1)(-1)(-1) = 1 \qquad \left(\frac{-3}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) = (1)(1) = 1$

$\left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = (1)(-1) = -1 \qquad \left(\frac{-1}{13}\right) = 1$

$\left(\frac{1}{13}\right) = 1^{\frac{13-1}{2}} = 1^6 = 1$ $\qquad$ $\left(\frac{2}{13}\right) = -1$

$\left(\frac{3}{13}\right) = 1$ $\qquad$ $\left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = (-1)(-1) = 1$

$\left(\frac{5}{13}\right) = -1$ $\qquad$ $\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (-1)(1) = -1$

So the primes p for which $x^2 \equiv 13 \pmod{p}$ has solutions are those that are congruent, mod 13, to $-4, -3, -1, 1, 3$, or 4. Or, if you prefer, those congruent to $1, 3, 4, 9, 10$, or 12.

29. If $p \geq 7$ is an odd prime, then $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right)$ for at least one of $n = 2, 3$, or 8.

Since $\left(\frac{n}{p}\right) = \pm 1$, it is enough to show that $\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \left(\frac{n(n+1)}{p}\right) = 1$ for at least one of these values. That is, we wish to show that one of $\left(\frac{6}{p}\right)$, $\left(\frac{12}{p}\right)$, or $\left(\frac{72}{p}\right)$ is 1.

But $\left(\frac{6}{p}\right) = \left(\frac{2 \cdot 3}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1$ when $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$ have the same sign. $\left(\frac{12}{p}\right) = \left(\frac{2^2 \cdot 3}{p}\right) = (\left(\frac{2}{p}\right))^2\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) = 1$ when, well, $\left(\frac{3}{p}\right) = 1$. $\left(\frac{72}{p}\right) = \left(\frac{2^3 \cdot 3^2}{p}\right) = (\left(\frac{2}{p}\right))^3(\left(\frac{3}{p}\right))^2 = \left(\frac{2}{p}\right) = 1$ when $\left(\frac{2}{p}\right) = 1$.

So, if $\left(\frac{2}{p}\right) = 1$, then $\left(\frac{8}{p}\right) = \left(\frac{9}{p}\right)$. If $\left(\frac{3}{p}\right) = 1$, then $\left(\frac{3}{p}\right) = \left(\frac{4}{p}\right)$. If neither of these cases occur, then both are -1, so $\left(\frac{2}{p}\right) = -1 = \left(\frac{3}{p}\right)$. So $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right)$ for at least one of $n = 2, 3$, or 8 .

30. Compute $\left(\frac{35}{149}\right)$, $\left(\frac{39}{145}\right)$, and $\left(\frac{280}{351}\right)$.

Let's treat these as Jacobi symbols, to speed up the computations.

$$\left(\frac{35}{149}\right) = \left(\frac{149}{35}\right)(-1)^{\frac{149-1}{2}\frac{35-1}{2}} = \left(\frac{35 \cdot 4 + 9}{35}\right)(-1)^{74 \cdot 17} = \left(\frac{9}{35}\right) = (\left(\frac{3}{35}\right))^2 = 1$$

$$\left(\frac{39}{145}\right) = \left(\frac{145}{39}\right)(-1)^{\frac{145-1}{2}\frac{39-1}{2}} = \left(\frac{39 \cdot 3 + 28}{39}\right)(-1)^{72 \cdot 19} = \left(\frac{28}{39}\right) = (\left(\frac{2}{39}\right))^2\left(\frac{7}{39}\right) =$$
$$\left(\frac{7}{39}\right) = \left(\frac{39}{7}\right)(-1)^{\frac{39-1}{2}\frac{7-1}{2}} = \left(\frac{7 \cdot 5 + 4}{7}\right)(-1)^{19 \cdot 3} = -\left(\frac{4}{7}\right) = -(\left(\frac{2}{7}\right))^2 = -1$$

$$\left(\frac{280}{351}\right) = \left(\frac{2^3 \cdot 35}{351}\right) = (\left(\frac{2}{351}\right))^3\left(\frac{35}{351}\right) = ((-1)^{\frac{351^2-1}{8}})^3\left(\frac{35}{351}\right) = ((-1)^{\frac{(-1)^2-1}{8}})^3\left(\frac{35}{351}\right) =$$
$$\left(\frac{35}{351}\right) = \left(\frac{351}{35}\right)(-1)^{\frac{351-1}{2}\frac{35-1}{2}} = \left(\frac{35 \cdot 10 + 1}{35}\right)(-1)^{175 \cdot 17} = \left(\frac{1}{35}\right)(-1) = -1$$