Math 445 Homework 7 Solutions

25. Show that 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, $\text{ord}_p(a) = p-1$, 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 $\left(\frac{a}{p}\right) = -1$.

26. The primes p for which $x^2 \equiv 7 \pmod{p}$ has solutions consists precisely of those primes lying in certain congruence classes mod 28 ; which ones?

We want to know for which primes p is $\left(\frac{7}{p}\right) = 1$. But by reciprocity,
$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)(-1)^{\frac{7-1}{2}\frac{p-1}{2}} = \left(\frac{p}{7}\right)(-1)^{3\frac{p-1}{2}} == \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}}$, which is
$\left(\frac{p}{7}\right)$ if $p \equiv 1 \pmod{4}$, and is $-\left(\frac{p}{7}\right)$ if $p \equiv 3 \pmod{4}$. So
$\left(\frac{7}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{7}\right) = 1$ and $p \equiv 1 \pmod{4}$, <u>or</u> $\left(\frac{p}{7}\right) = -1$ and $p \equiv 3 \pmod{4}$.

But the value of $\left(\frac{p}{7}\right)$ depends only on p mod 7, and half of the congruence classes (and 0) will contain squares. And we can find these by inspection:
$1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2 \pmod{7}$, and so $\left(\frac{p}{7}\right) = 1$ for $p \equiv 1, 2, 4 \pmod{7}$. The remaining congruence classes, $p \equiv 3, 5, 6 \pmod{7}$, yield primes with $\left(\frac{p}{7}\right) = -1$.

So, $\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$ and $p \equiv 1, 2,$ or $4 \pmod{7}$, <u>or</u> $p \equiv 3 \pmod{4}$ and $p \equiv 3, 5,$ or $6 \pmod{7}$, [together with 2 and 7].
But each of these six possibilities represents a single congruence class mod 28, by the chinese remainder theorem, e.g., $p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{7} \Leftrightarrow p \equiv 1 \pmod{28}$. Rather than work through the procedure as the proof of CRT would, we can use the fact that we know there is one congruence class mod 28 containing the solutions to the simultaneous equations $p \equiv a$ mod 4,$p \equiv b$ mod 7, we can find representatives experimentally.
Writing some of the integers $\equiv 1 \pmod{4}$, $n = 1, 5, 9, 13, 17, 21, 25, 29$, we note that $1 \equiv 1 \pmod{7}$, $9 \equiv 2 \pmod{7}$, and $25 \equiv 4 \pmod{7}$, so
$p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{7} \Leftrightarrow p \equiv 1 \pmod{28}$ $p \equiv 1 \pmod{4}$ and $p \equiv 2 \pmod{7} \Leftrightarrow p \equiv 9 \pmod{28}$ $p \equiv 1 \pmod{4}$ and $p \equiv 4 \pmod{7} \Leftrightarrow p \equiv 25 \pmod{28}$
Similarly, writing some of the integers $\equiv 3 \pmod{4}$, $n = 3, 7, 11, 15, 19, 23, 27, 31$, we note that $3 \equiv 3(mod 7)$, $19 \equiv 5 \pmod{7}$, and $27 \equiv 6 \pmod{7}$, so
$p \equiv 3 \pmod{4}$ and $p \equiv 3 \pmod{7} \Leftrightarrow p \equiv 3 \pmod{28}$ $p \equiv 3 \pmod{4}$ and $p \equiv 5 \pmod{7} \Leftrightarrow p \equiv 19 \pmod{28}$ $p \equiv 3 \pmod{4}$ and $p \equiv 6 \pmod{7} \Leftrightarrow p \equiv 27 \pmod{28}$

So the primes p with $\left(\frac{7}{p}\right) = 1$ are precisely those congruent to one of 1,3,9,19,25, or 27 (mod 28). [To be formally complete, we should add the classes 2 and 7, each containing a single prime (2 and 7).]

27. Compute the (Jacobi) symbols $\left(\frac{31}{113}\right)$ and $\left(\frac{131}{311}\right)$.

$\left(\frac{31}{113}\right)\left(\frac{113}{31}\right) = (-1)^{\frac{31-1}{2}\frac{113-1}{2}} = (-1)^{15\cdot 56} = 1$, so $\left(\frac{31}{113}\right) = \left(\frac{113}{31}\right) = \left(\frac{31\cdot 3+20}{31}\right) = \left(\frac{20}{31}\right) = \left(\frac{2^2 5}{31}\right) = \left(\frac{2}{31}\right)^2\left(\frac{5}{31}\right) = 1\cdot\left(\frac{5}{31}\right) = \left(\frac{5}{31}\right)$, since whatever $\left(\frac{2}{31}\right)$ is, its square will be 1.

But now $\left(\frac{5}{31}\right)\left(\frac{31}{5}\right) = (-1)^{\frac{5-1}{2}\frac{31-1}{2}} = (-1)^{2\cdot 15} = 1$, so $\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right) = \left(\frac{6\cdot 5+1}{5}\right) = \left(\frac{1}{5}\right) = 1$, since thinking of this as a Legendre symbol, $1 = 1^2$ is a square mod 5.

So, put together, $\left(\frac{31}{113}\right) = \left(\frac{113}{31}\right) = \left(\frac{5}{31}\right) = \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$, so $\left(\frac{31}{113}\right) = 1$.

For $\left(\frac{131}{311}\right)$, we have $\left(\frac{131}{311}\right)\left(\frac{311}{131}\right) = (-1)^{\frac{131-1}{2}\frac{311-1}{2}} = (-1)^{65\cdot 155} = -1$, so $\left(\frac{131}{311}\right) = -\left(\frac{311}{131}\right) = -\left(\frac{2\cdot 131+49}{131}\right) = -\left(\frac{49}{131}\right) = -\left(\frac{7^2}{131}\right) = -\left(\frac{7}{131}\right)^2 = -1$, since $\left(\frac{7}{131}\right) = \pm 1$, so its square is 1.

So $\left(\frac{131}{311}\right) = -\left(\frac{311}{131}\right) = -1$.

28. [NZM, p.137, # 19] Show that for every (odd) prime p, the residue equation

$$x^8 \equiv 16 \pmod{p}$$

always has a solution.

By our more ancient criterion, for p an (odd) prime and (hence) $(16, p) = 1$, $x^8 \equiv 16 \pmod{p}$ has a solution $\Leftrightarrow 16^{\frac{p-1}{(8,p-1)}} \equiv 1 \pmod{p}$; we wish to show that this latter is always true. But since $16 = 2^4$, this means that we wish to show that
$(2^4)^{\frac{p-1}{(8,p-1)}} = 2^{4\cdot\frac{p-1}{(8,p-1)}} \equiv 1$.
But we know that $2^{p-1} \equiv 1 \pmod{p}$, so what we wish to show is true <u>is</u> true if
$p-1 | 4\cdot\frac{p-1}{(8,p-1)}$, i.e., $4\cdot\frac{p-1}{(8,p-1)} = (p-1)n$ for some integer n, i.e.,
$4\cdot(p-1) = (p-1)n(8,p-1)$, i.e., $4 = n(8,p-1)$ for some n, i.e., $(8,p-1)|4$.
But since p is odd, $p = 8k + r$ for some k and for $r =$ one of 1,3,5, or 7, and so
$p - 1 = 8k + (r-1)$. So $(8, p-1) = (8, 8k + (r-1)) = (8, r-1)$, so $(8, p-1) =$ one of $(8,0) = 8$, $(8,2) = 2$, $(8,4) = 4$, or $(8,6) = (2,6) = 2$. So in every case except $r = 1$ (so $p \equiv 1 \pmod{8}$) we have $(8, p-1)|4$, as desired, so we have shown:
(*) unless $p \equiv 1 \pmod{8}$, $x^8 \equiv 16 \pmod{p}$ has a solution.

But! if p is prime and $p \equiv 1 \pmod{8}$, then $x^2 \equiv 2 \pmod{p}$ has a solution; $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ and $\frac{p^2-1}{8}$ is even. So, for that value of x, $x^8 = (x^2)^4 \equiv 2^4 = 16$, so $x^8 \equiv 16 \pmod{p}$ has a solution, as desired.

So, for every odd prime p, $x^8 \equiv 16 \pmod{p}$ has a solution.