

book problems

§8.2 #1

a). There exist at most 2 incongruent solutions to $x^2 \equiv 1 \pmod{p}$ by Lagrange's Theorem. Since 1 and $p-1$ are incongruent and both satisfy $x^2 \equiv 1 \pmod{p}$, these are the only two solutions.

b). $x^{p-1} - 1 = (x-1)(x^{p-2} + \dots + x^2 + x + 1)$. Hence any solutions to $x^{p-1} - 1 \equiv 0 \pmod{p}$ which is not a solution to $x-1 \equiv 0 \pmod{p}$ must be a solution to $x^{p-2} + \dots + x^2 + x + 1 \equiv 0 \pmod{p}$. Since $1, 2, \dots, p-1$ are all solutions to $x^{p-1} - 1 \equiv 0 \pmod{p}$, we see that $2, 3, \dots, p-1$ are solutions to $x^{p-2} + \dots + x^2 + x + 1 \equiv 0 \pmod{p}$. By Lagrange's theorem this is all of the solutions.

§8.2 #8. Let r be a primitive root of p , p odd.

a). Assume $p \equiv 1 \pmod{4}$. Show $-r$ has order $p-1$. Let $h = o(-r) \pmod{p}$. Then $h \mid p-1$. Since $p \equiv 1 \pmod{4}$, $\frac{p-1}{2}$ is even. Thus $(-r)^{(p-1)/2} \equiv r^{(p-1)/2}$ which is not congruent to 1 \pmod{p} . Therefore $h \nmid \frac{p-1}{2}$ and as a consequence h is even. Therefore $(-r)^h = r^h \equiv 1 \pmod{p}$ and hence $h = p-1$ since that is the order of r .

b). Assume $p \equiv 3 \pmod{4}$. Show $-r$ has order $\frac{p-1}{2}$. Since $p \equiv 3 \pmod{4}$, $\frac{p-1}{2}$ is odd. Now $(-r)^{(p-1)/2} = (-1)r^{(p-1)/2}$. And since $r^{(p-1)/2}$ satisfies $x^2 \equiv 1 \pmod{p}$, by problem 1, either $r^{(p-1)/2} \equiv 1 \pmod{p}$ or $r^{(p-1)/2} \equiv -1 \pmod{p}$. Since r has order $p-1$ it must be the latter. Therefore $(-r)^{(p-1)/2} \equiv 1 \pmod{p}$. Let $h = o(-r) \pmod{p}$. By what we have shown $h \mid \frac{p-1}{2}$. Therefore h is odd. Therefore $(-r)^h = (-1)r^h \equiv 1 \pmod{p}$. Thus $r^h \equiv -1 \pmod{p}$ and we see that $(r^h)^2 \equiv 1 \pmod{p}$. This implies $2h = p-1$. Therefore $h = \frac{p-1}{2}$.