ELEMENTARY NUMBER THEORY

HOMEWORK 5

These are problems I will be going through next Tuesday. Solve as many as you can, but at least four.

(1) Use Gauss's Lemma to prove that $(\frac{-2}{p}) = +1$ or -1 according as $p \equiv 1, 3 \bmod 8$ or $p \equiv 5, 7 \bmod 8$.

Assume first that $p = 4n + 1$. Then $A = \{1, 2, \ldots, 2n\}$ is a half system (every integer coprime to p is congruent either to a number in A or to a number in $-A$). Multiplying through by -2 gives (all congruences mod p):

$$\begin{aligned} -2 \cdot 1 &\equiv -2, \\ -2 \cdot 2 &\equiv -4, \\ &\vdots \\ -2 \cdot n &\equiv -2n, \\ -2 \cdot (n+1) &\equiv -2n - 2 \equiv 2n - 1, \\ &\vdots \\ -2 \cdot 2n &\equiv -4n \equiv 1. \end{aligned}$$

There are exactly n minus signs on the right, hence $(\frac{-2}{p}) = (-1)^n$. Now there are two cases:

(a) $n = 2k$ is even: then $p = 4n + 1 = 8k + 1 \equiv 1 \bmod 8$, and $(\frac{-2}{p}) = (-1)^{2k} = +1$.

(b) $n = 2k + 1$ is even: then $p = 4n + 1 = 8k + 5 \equiv 5 \bmod 8$, and $(\frac{-2}{p}) = (-1)^{2k+1} = -1$.

Here are the calculations for $p = 4n + 3$: $A = \{1, 2, \ldots, 2n + 1\}$ is a half system, and we get

$$\begin{aligned} -2 \cdot 1 &\equiv -2, \\ -2 \cdot 2 &\equiv -4, \\ &\vdots \\ -2 \cdot n &\equiv -2n, \\ -2 \cdot (n+1) &\equiv -2n - 2 \equiv 2n + 1, \\ &\vdots \\ -2 \cdot (2n+1) &\equiv -4n - 2 \equiv 1. \end{aligned}$$

Again we find $(\frac{-2}{p}) = (-1)^n$, and there are two cases:

(a) $n = 2k$ is even: then $p = 4n + 3 = 8k + 3 \equiv 3 \bmod 8$, and $(\frac{-2}{p}) = (-1)^{2k} = +1$.
(b) $n = 2k + 1$ is even: then $p = 4n + 3 = 8k + 7 \equiv 7 \bmod 8$, and $(\frac{-2}{p}) = (-1)^{2k+1} = -1$.

(2) Show that $\sum_{a=1}^{p-1}(\frac{a}{p}) = 0$.

This is clear since half of the residue classes in $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares, an half are nonsquares.

Here is a second proof: let n be a nonsquare mod p; then

$$\left(\frac{n}{p}\right)\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = \sum_{a=1}^{p-1}\left(\frac{an}{p}\right) = \sum_{b=1}^{p-1}\left(\frac{b}{p}\right).$$

This is because is a through $(\mathbb{Z}/p\mathbb{Z})^\times$, then so does $b = na$ (we used this in our proof of Fermat's Little Theorem). Thus the sum in question does not change when we multiply it by $(\frac{n}{p}) = -1$, hence it must be 0.

(3) Let $p = a^2 + 4b^2$ be a prime. Show that $(\frac{a}{p}) = +1$.

Observe that $p \equiv a^2 \equiv 1 \bmod 4$ since a is odd. Thus, by the reciprocity law, $(\frac{a}{p}) = (\frac{p}{a}) = (\frac{4b^2}{a}) = +1$ since $p \equiv 4b^2 \bmod a$ and since $4b^2$ is a square.

(4) Show that, for Fermat primes $p = F_n = 2^{2^n} + 1$, we have $\phi(p-1) = \frac{p-1}{2}$. Conclude that every quadratic nonresidue mod p is a primitive root mod p.

Clearly $\phi(p-1) = \phi(2^{2^n}) = 2^{2^{n-1}} = \frac{p-1}{2}$. We know that there are $\phi(p-1)$ primitive roots, an that every primitive root is a quadratic nonresidue. But there are exactly $\frac{p-1}{2}$ nonresidues, hence every nonresidue automatically is a primitive root.

(5) Show that 3 is a primitive root modulo p for every for every Fermat prime F_n with $n > 0$.

All we need to do is show that 3 is a quadratic nonresidue mod F_n. But $F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \equiv 2 \bmod 3$ and $F_n \equiv 1 \bmod 4$, hence $(3/F_n) = (F_n/3) = (2/3) = -1$.

(6) Let $n = 4m^2 + 3$, where m is an integer not divisible by 3. Show that there exists a prime $p \mid n$ with $p \equiv 7 \bmod 12$.

Let $p \mid n$; then $-3 \equiv 4m^2 \bmod p$ tells us that $(\frac{-3}{p}) = +1$ (note that $3 \nmid m$), and the quadratic reciprocity law says $(\frac{-3}{p}) = (\frac{p}{3})$. Thus $p \equiv 1 \bmod 3$ for every such p.

On the other hand, $n \equiv 3 \bmod 4$, so there must be a prime factor of the form $p \equiv 3 \bmod 4$. We have seen $p \equiv 1 \bmod 3$, and the Chinese remainder theorem then shows that $p \equiv 7 \bmod 12$.

(7) Show that there are infinitely many primes $p \equiv 7 \bmod 12$.

Assume you have primes $p_1 = 7, p_2, \ldots, p_n$ all $\equiv 7 \bmod 12$. Let $N = 4(p_1 \cdots p_n)^2 + 3$. There is a prime $p \equiv 7 \bmod 12$ dividing N. Also, $p \neq p_k$

since $p_k \mid (N-1)$, hence $p_k \nmid N$. Thus $p \equiv 7 \bmod 12$ is a prime not on our list.