Math 40520 Theory of Number
Homework 6

Due Wednesday, 2015-10-07, in class

Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.

1. Let $p > 3$ be a prime number and write $P = \{1, 2, \dots, (p-1)/2\}$. Show that $x \in P$ is such that

$$3x \in 3P \cap (-P)$$

if and only if

$$\left\lceil \frac{p+1}{6} \right\rceil \leq x \leq \left\lfloor \frac{p-1}{3} \right\rfloor$$

and conclude that for $p > 3$,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Proof. Note that if $x \leq (p-1)/3$ then $3x \leq p-1$ so $3x$ is its residue mod p. When $x > (p-1)/3$ then the residue of $3x$ mod p is $3x - p$ as then $0 \leq 3x - p < p$ given that $3x < 3(p-1)/2 < p$. In fact $3x - p < (p+1)/2$ so for such x, $3x \notin -P$. Therefore we only need to count those $x \leq (p-1)/3$ such that $3x \in -P = \{(p+1)/2, \dots, p-1\}$, i.e., $(p+1)/3 \leq 3x \leq p-1$. This is equivalent to the condition in the problem.

Gauss' Lemma implies that $\left(\frac{3}{p}\right) = (-1)^{|3P \cap -P|}$ and the previous result shows that the exponent equals the number of x such that $\lceil \frac{p+1}{6} \rceil \leq x \leq \lfloor \frac{p-1}{3} \rfloor$, namely

$$N_p = \left\lfloor \frac{p-1}{3} \right\rfloor - \left\lceil \frac{p+1}{6} \right\rceil + 1$$

We only need to determine whether this number is even or odd. Note that adding a multiple of 12 to p doesn't change the parity of this number so it suffices to determine its parity for the residues of p mod 12. As $p > 3$ its residue mod 12 is $1, 5, 7, 11$ and we just check that the values we get are $N_1 = 0$, $N_5 = 1$, $N_7 = 1$ and $N_{11} = 2$ and the result follows. $\square$

2. Let $p > 5$ be a prime number and write $P = \{1, 2, \dots, (p-1)/2\}$. Show that $x \in P$ is such that

$$5x \in 5P \cap (-P)$$

if and only if

$$\left\lceil \frac{p+1}{10} \right\rceil \leq x \leq \left\lfloor \frac{p-1}{5} \right\rfloor \text{ or } \left\lceil \frac{3p+1}{10} \right\rceil \leq x \leq \left\lfloor \frac{2p-1}{5} \right\rfloor$$

and conclude that for $p > 5$,

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 9 \pmod{20} \\ -1 & \text{if } p \equiv \pm 3, \pm 7 \pmod{20} \end{cases}$$

and remark that this is equivalent to the simpler statement

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{5} \\ -1 & \text{if } p \equiv \pm 2 \pmod{5} \end{cases}$$

Proof. If $x \leq (p-1)/5$ then the residue of $5x$ is $5x$. if $(p-1)/5 < x < (2p-1)/5$ then the residue of $5x$ is $5x-p$ as then $0 \leq 5x-p \leq p-1$. Finally, if $(2p-1)/5 < x \leq (p-1)/2$ then the residue of $5x$ mod p is $5x-2p$. Note that in that case $0 \leq 5x-2p \leq 5(p-1)/2-2p < (p+1)/2$ so the only way $5x \mod p \in -P$ is if $x \leq (p-1)/5$ and the integer $5x \geq (p+1)/2$ or if $(p-1)/5 < x \leq (2p-1)/5$ and the integer $5x-p \geq (p+1)/2$. These are equivalent to $(p+1)/10 \leq x \leq (p-1)/5$ or $(3p+1)/10 \leq x \leq (2p-1)/5$. This yields the first part of the problem.

For the second part, again Gauss' Lemma implies that $\left(\frac{5}{p}\right) = (-1)^{|5P \cap (-P)|} = (-1)^{N_p}$ where

$$N_p = \left\lfloor \frac{2p-1}{5} \right\rfloor - \left\lceil \frac{3p+1}{10} \right\rceil + 1 + \left\lfloor \frac{p-1}{5} \right\rfloor - \left\lceil \frac{p+1}{10} \right\rceil + 1$$

Again the parity doesn't change if we add multiples of 20 to p and so it suffices to verify the parity of N_p for the residues $p \mod 20$ which can be $1, 3, 7, 9, 11, 13, 17, 19$. The values for these residues are $N_1 = 0$, $N_3 = 1$, $N_7 = 1$, $N_9 = 2$, $N_{11} = 2$, $N_{13} = 3$, $N_{17} = 3$, $N_{19} = 4$ and the result follows $\mod 20$. The result mod 5 is immediate as $\pm 1, \pm 9 \mod 20$ is equivalent to $\pm 1 \mod 5$. $\square$

3. Let $p > 3$ be a prime number $\equiv 2 \pmod{3}$. Show that $p \mid x^2 + 3y^2$ for integers x and y if and only if $p \mid x$ and $p \mid y$. [Hint: Use Problem 1.]

   Proof. Suppose $p \mid x^2 + 3y^2$. As $p > 3$, $p \mid x$ if and only if $p \mid y$. Suppose now that $x, y \in \mathbb{Z}_p^{\times}$. Then $x^2 + 3y^2 \equiv 0 \pmod{p}$ implies $-3 = (x/y)^2 \pmod{p}$ so -3 is a square mod p. But then

   $$\left(\frac{-3}{p}\right) = 1$$

   and we compute

   $$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

   Since $p \equiv 2 \pmod{3}$ it follows that $p \equiv 5, 11 \pmod{12}$. If $p \equiv 5 \pmod{12}$ it follows that $p \equiv 1 \pmod{4}$ so $\left(\frac{-1}{p}\right) = 1$ while the first problem implies that $\left(\frac{3}{p}\right) = -1$. We deduce that $\left(\frac{-3}{p}\right) = -1$, a contradiction. If $p \equiv 11 \pmod{12}$ it follows that $p \equiv 3 \pmod{4}$ so $\left(\frac{-1}{p}\right) = -1$ whereas the first problem implies that $\left(\frac{3}{p}\right) = 1$ again yielding the contradiction $\left(\frac{-3}{p}\right) = -1$.

   $\square$

4. Let p be an odd prime. Suppose that $a \neq 0$ is a square mod p. Show that a is a square mod p^n for every $n \geq 1$.

Proof. If $P(x) = x^2 - a \equiv 0 \pmod p$ has a root α then $\alpha \not\equiv 0 \pmod p$ and so $P'(\alpha) = 2\alpha \not\equiv 0 \pmod p$ (as p is odd). Then Hensel's lemma implies that $P(x) \equiv 0 \pmod{p^n}$ always has roots. $\square$

5. Let a be an odd integer and $n \geq 3$ be an integer. Show that a is a square modulo 2^n if and only if $a \equiv 1 \pmod 8$. [Hint: In class we showed that 17 is a square mod 2^n and indeed $17 \equiv 1 \pmod 8$.]

Proof. As $8 \mid 2^n$ if $x^2 \equiv a \pmod{2^n}$ we get that $x^2 \equiv a \pmod 8$. The only odd square modulo 8 is 1, by inspection, as $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1 \pmod 8$. Reciprocally, suppose that $a = 1 + 8k$. We need to solve the congruence $x^2 \equiv 1 + 8k \pmod{2^n}$. A solution would necessarily be odd and writing $x = 2y + 1$ this is equivalent to

$$4y^2 + 4y + 1 \equiv 1 + 8k \pmod{2^n}$$

which is equivalent to

$$y^2 + y - 2k \equiv 0 \pmod{2^{n-2}}$$

It suffices to show that this equation has roots for all $m = n - 2 \geq 1$. Mod 2 the equation has the root $y = 0$. Hensel's lemma applies as $Q'(y) = 2y + 1 = 1 \pmod 2$ doesn't vanish and so $Q(y) \equiv 0 \pmod{2^m}$ always has roots. $\square$

6. Let $p > 2$ be a prime and $k, n \geq 1$ be two integers. Show that there are $\dfrac{\varphi(p^n)}{(k, \varphi(p^n))}$ residues in $\mathbb{Z}_{p^n}^\times$ which are k-th powers.

Proof. As p is odd, $\mathbb{Z}_{p^n}^\times$ is cyclic with some primitive root g. Then we need to count those $a = g^r$ such that the equation $(g^s)^k \equiv g^r \pmod{p^n}$ has a solution with $0 \leq s < \varphi(p^n)$. As g has order $\varphi(p^n)$ this is equivalent to $ks \equiv r \pmod{\varphi(p^n)}$. This equation has a solution with s integral if and only if there exists an integer M such that

$$ks = r + \varphi(p^n)M$$

Immediately if such s and M exist then

$$d = (k, \varphi(p^n)) \mid r = ks - \varphi(p^n)M$$

Suppose that $d \mid r$. Then k/d and $\varphi(p^n)/d$ are coprime integers whereas r/d is an integer. Therefore the equation

$$(k/d)s \equiv r/d \pmod{\varphi(p^n)/d}$$

has a solution (since k/d is invertible modulo $\varphi(p^n)/d$). We can therefore find an integer M such that

$$(k/d)s = r/d + \varphi(p^n)/d \cdot M$$

which immediately yields a solution to the congruence $ks \equiv r \pmod{\varphi(p^n)}$.

Therefore we need to count the r such that $0 \leq r < \varphi(p^n)$ such that $d \mid r$. Then r is of the form $r = du$ where $0 \leq u < \varphi(p^n)/d$ and there are exactly $\varphi(p^n)/d$ such integers. $\square$

7. Exercise 7.27 on page 141.

Proof. Recall from class that exactly half the residues in $\mathbb{Z}_p^\times$ are squares. Thus half the legendre symbols are 1, the other half being -1, which implies the total sum is 0. The second part we did in class. Indeed, the quadratic residues are the even powers of a primitive element so

$$\sum_{a \in Q_p} a = 1 + g^2 + g^4 + \cdots + g^{p-3} = \frac{g^{p-1} - 1}{g^2 - 1} = 0$$

as $g^2 - 1 \neq 0$ since $p > 3$. $\square$

8. (A simplification of Exercise 7.22 to not necessitate quadratic reciprocity) Suppose q and r are distinct primes such that $q \equiv r \equiv 1 \pmod 4$ and $\left(\frac{q}{r}\right) = \left(\frac{r}{q}\right) = 1$. Show that $(x^2 - q)(x^2 - r)(x^2 - qr) = 0$ has no rational solutions but has solutions modulo n for every positive integer n. [Hint: You might find Problem 5 useful.]

Proof. The equation has roots $\pm\sqrt{q}, \pm\sqrt{r}$, and $\pm\sqrt{qr}$ which are not rational. By the CRT it is enough to show that the equation has roots mod p^k for all primes p and $k \geq 1$.

Suppose $p \notin \{2, q, r\}$. Then one of $\left(\frac{q}{p}\right), \left(\frac{r}{p}\right), \left(\frac{qr}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{r}{p}\right)$ is 1 (as $(-1) \cdot (-1) = 1$). Thus one of the equations $x^2 - q = 0$, $x^2 - r = 0$ and $x^2 - qr = 0$ has solutions mod p. Any solution $x = x_0$ will then be $\not\equiv 0 \pmod p$ as that would imply that q, r or qr is divisible by p. Moreover, as $p \neq 2$, Hensel's lemma implies the existence of a root of the appropriate quadratic modulo p^k for all k and therefore a solution of $P(x) = (x^2 - q)(x^2 - r)(x^2 - qr) \equiv 0 \pmod{p^k}$.

If $p = q$ then the above argument yields roots of $x^2 - r \equiv 0 \pmod{q^k}$ for all k because r is a square mod q and we can still apply Hensel's lemma as $r \neq q$. A similar argument works if $p = r$.

Finally, we treat the case $p = 2$. We need solutions of $P(X) \equiv 0 \pmod{2^k}$ for all k large enough and let's suppose that $k \geq 3$. Problem 5 guarantees a root of $x^2 - a \equiv 0 \pmod{2^k}$ as long as $a \equiv 1 \pmod 8$. If q or r is $\equiv 1 \pmod 8$ then we have a root mod 2^k of $x^2 - q$ or $x^2 - r$. Otherwise $q, r \equiv 5 \pmod 8$. But then $qr \equiv 5^2 \equiv 1 \pmod 8$ and so $x^2 - qr$ has roots mod 2^k. $\square$