FINAL EXAM SOLUTIONS
MATH 115: NUMBER THEORY

Problem 1. The congruence implies that $p^k \mid (x^2-1) = (x-1)(x+1)$. Now, if p is an odd prime such that $p \mid (x-1)$ and $p \mid (x+1)$, then $p \mid (x-1)+(x+1) = 2x$ so since p is odd, $p \mid x$. Thus $p \mid x-(x-1) = 1$, a contradiction. Therefore either $p^k \mid (x-1)$ or $p^k \mid (x+1)$, hence $x \equiv \pm 1 \pmod{p^k}$.

Alternatively, we know that $f(x) = x^2 - 1 \equiv 0 \pmod p$ which has only the solutions $x \equiv \pm 1 \pmod p$; by Hensel's lemma, since $f'(\pm 1) = \pm 2 \not\equiv 0 \pmod p$, these lift uniquely, so there are exactly two solutions modulo p^k, hence they must be $x \equiv \pm 1 \pmod{p^k}$.

[N.B. There is also a solution which uses the fact that p^k has a primitive root!]

Problem 2. First, the congruence has the solution $x \equiv 1 \pmod 3$ for $p = 3$. Now assume $p \neq 3$, so that $x \equiv 1 \pmod p$ is not a solution. Note that

$$(x-1)(x^2+x+1) = x^3 - 1 \equiv 0 \pmod p.$$

Therefore the original congruence has a solution if and only if there is a nontrivial solution to this congruence, i.e. an element of order 3. This happens if and only if $3 \mid (p-1)$, i.e. $p \equiv 1 \pmod 3$.

Alternatively, note that by a homework exercise (completing the square), the original congruence has a solution if and only if $y^2 \equiv d \equiv 1^2 - 4(1)(1) = -3 \pmod p$ has a solution. This has the solution $y \equiv 0 \pmod 3$ if $p = 3$, and otherwise, we need $(-3/p) = 1$, which again by a homework exercise (using quadratic reciprocity) we see that $p \equiv 1 \pmod 3$.

Problem 3. We note that

$$\sigma(n) = \sigma(pq) = (p+1)(q+1) = pq + p + q + 1 = 51809 + p + q + 1 = 52416,$$

so $p + q = 606$. Thus p, q are the roots of

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - 606x + 51809 = 0$$

so

$$p, q = \frac{606 \pm \sqrt{606^2 - 4(51809)}}{2} = 303 \pm 200 = 103, 503.$$

Problem 4. For (a), suppose $m, n \in \mathbb{Z}_{\geq 1}$ with $\gcd(m, n) = 1$. Note that

$$f(mn) = (-1)^{mn-1}$$

and

$$f(m)f(n) = (-1)^{m-1}(-1)^{n-1} = (-1)^{(m-1)+(n-1)} = (-1)^{m+n}$$

hence we need to show that

$$mn - 1 \equiv m + n \pmod 2.$$

Date: August 12, 2004.

Since $\gcd(m,n) = 1$, not both of m, n are even. Without loss of generality, then, we may assume $m \equiv 0, 1 \pmod 2$ and $n \equiv 1 \pmod 2$. The congruence is true in both of these cases.

For (b), the easiest method is to use the homework: if $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_r)).$$

Now if one p_i is odd, then $f(p_i) = 1$ so the sum is zero.

To essentially reprove this result, argue as follows: since f is multiplicative and μ is multiplicative, so is their product μf. Therefore, since g is the summatory function of μf, so is g.

So suppose $n = p^e$ is an odd prime power, $e \geq 1$. Then

$$\begin{aligned} g(p^e) &= \sum_{d|p^e} \mu(p^e) f(p^e) = \mu(1)f(1) + \mu(p)f(p) + \cdots + \mu(p^e)f(p^e) \\ &= f(1) + f(p) = (-1)^{1-1} - (-1)^{p-1} = 1 - 1 = 0 \end{aligned}$$

since p is odd.

Now suppose that n is not a power of 2. Then there is an odd prime p which divides n. Write $n = p^e m$ where $p \nmid m$. Then by multiplicativity,

$$g(n) = g(p^e)g(m) = 0.$$

Problem 5. We first note that $p \equiv 1 \pmod 4$. This follows since

$$p \equiv a^2 + 5b^2 \equiv a^2 + b^2 \equiv 0, 1, 2 \pmod 4$$

but p is an odd prime, so $p \equiv 1 \pmod 4$.

Therefore by quadratic reciprocity, since a is an odd prime,

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2 + 5b^2}{a}\right)$$

and since $a^2 + 5b^2 \equiv 5b^2 \pmod a$, and $(b^2/a) = 1$ clearly, we have

$$\left(\frac{a^2 + 5b^2}{a}\right) = \left(\frac{5b^2}{a}\right) = \left(\frac{5}{a}\right)\left(\frac{b^2}{a}\right) = \left(\frac{5}{a}\right)$$

which by quadratic reciprocity is

$$\left(\frac{5}{a}\right) = \left(\frac{a}{5}\right).$$

Therefore a is a quadratic residue modulo p if and only if $\left(\frac{a}{5}\right) = 1$. This latter holds if and only if $a \equiv \pm 1 \pmod 5$, which implies that

$$p \equiv a^2 \equiv 1 \pmod 5.$$

Problem 6. By Euler's theorem, we note that

$$a^{\phi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}.$$

Therefore since $\phi(p_i^{e_i}) \mid m$, we have

$$a^m \equiv 1 \pmod{p_i^{e_i}}.$$

By the Chinese remainder theorem, this implies that

$$a^m \equiv 1 \pmod n.$$

Therefore $o(a \bmod n) \mid m$. This solves (a).

For (b), the answer is "no". Indeed, if we take $n = 8 = 2^3$, there is no element of order $\phi(8) = 4$ modulo 8.

Problem 7. Note first that $p \nmid a$. Now since $o(-a^2 \bmod p) \mid p - 1 = 2q$, we have $o(-a^2 \bmod p) \in \{1, 2, q, 2q\}$.

First, suppose $o(-a^2 \bmod p) \mid 2$, so that

$$(-a^2)^2 \equiv a^4 \equiv 1 \pmod{p}.$$

Hence $o(a \bmod p) = 1, 2, 4$. If $o(a \bmod p) = 1, 2$, then $a^2 \equiv 1 \pmod{p}$, so $a \equiv \pm 1 \pmod{p}$, a contradiction. If $o(a \bmod p) = 4$, then $4 \mid (p-1)$ so $p \equiv 2q + 1 \equiv 1 \pmod{4}$, a contradition since q is odd.

Therefore we only need to rule out $o(-a^2 \bmod p) = q$. If so, then

$$(-a^2)^q \equiv -a^{2q} \equiv 1 \pmod{p}.$$

But $\phi(p) = p - 1 = 2q$, so by Fermat's little theorem, since $p \nmid a$, we know that $a^{2q} \equiv 1 \pmod{p}$. Therefore $-a^{2q} \equiv -1 \equiv 1 \pmod{p}$, a contradiction since p is odd. Thus $o(-a^2 \bmod p) = 2q = \phi(p)$, so $-a^2 \bmod p$ is a primitive root.

Problem 8 (Bonus). [N.B. Note that $\phi(1) = 1 = \sqrt{1}$, $\phi(4) = 2 = \sqrt{4}$ but $\phi(2) = 1 < \sqrt{2}$ and $\phi(6) = 2 < \sqrt{6}$.]

For any real number $x \geq 3$, we claim that

$$x - 1 > \sqrt{x}.$$

This follows since it is equivalent to

$$(x-1)^2 = x^2 - 2x + 1 > x$$

and this is equivalent to

$$f(x) = x^2 - 3x + 1 > 0.$$

Note that f is a continuous function; $f'(x) = 2x - 3 > 0$ for $x > 3/2$, so f is increasing there; so since $f(3) = 9 - 9 + 1 > 0$, $f(x) > 0$ for $x \geq 3$.

Now, suppose $n = p^e$ is an odd prime power, with $e \geq 1$. Then

$$\phi(p^e) = p^{e-1}(p-1) > p^{e-1}\sqrt{p}$$

and since $e - 1/2 \geq e/2$ (this is equivalent to $e/2 \geq 1/2$, or $e \geq 1$), we have

$$p^{e-1}\sqrt{p} = p^{e-1/2} \geq p^{e/2} = \sqrt{p^e}.$$

Finally, if n is odd, then

$$\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r}) > \sqrt{p_1^{e_1} \cdots p_r^{e_r}} = \sqrt{n}.$$

To conclude, one must treat the case that n is even! We leave it as a challenge to the reader to modify the above argument appropriately.