FINAL EXAM REVIEW SOLUTIONS
MATH 115: NUMBER THEORY

Problem 1. If p is odd, then without loss of generality, a is even and b is odd. Therefore

$$p = a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 4.$$

For (b), note that since $p \equiv 1 \pmod 4$ is prime and a is prime as well, by quadratic reciprocity,

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

Now the Legendre symbol only depends on the numerator modulo a, so since $a^2 + b^2 \equiv b^2 \pmod a$, we have

$$\left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1.$$

Problem 2. We compute using quadratic reciprocity:

$$\left(\frac{103}{229}\right) = \left(\frac{229}{103}\right) = \left(\frac{23}{103}\right) = -\left(\frac{103}{23}\right) = -\left(\frac{11}{23}\right) = \left(\frac{23}{11}\right) = \left(\frac{1}{11}\right) = 1.$$

Problem 3. Since $3^p + 1 \equiv 0 \pmod n$, we have $3^p \equiv -1 \pmod n$, hence $3^{2p} \equiv 1 \pmod n$. Therefore $h = o(3 \bmod n) \mid 2p$, hence $h \in \{1, 2, p, 2p\}$. If $h = 1$, then $3^1 = 3 \equiv 1 \pmod n$, so $n \mid (3-1) = 2$, but we see that $n \geq 28$, so this is impossible. Similarly, if $h = 2$, then $3^2 = 9 \equiv 1 \pmod n$, so $n \mid 8$, impossible. Finally, if $h = p$, then $3^p \equiv 1 \equiv -1 \pmod n$, which is again impossible. Therefore $h = o(3 \bmod n) = 2p$.

For (b), first note that the arguments above work with n replaced by q. We have the same congruences (except modulo q), and now we cannot have $3 \equiv 1 \pmod q$ or $9 \equiv 1 \pmod q$ since q is odd. So $o(3 \bmod q) = 2p$. Therefore $2p \mid (q-1)$, so $2pk = q - 1$, hence $q = 1 + 2pk$.

Problem 4. Let $n = p_1^{e_1} \cdots p_r^{e_r}$, with $e_i > 0$, p_i prime. Then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1) \mid 3p_1^{e_1} \cdots p_r^{e_r}.$$

Cancelling the common factors from both sides, we see this can happen if and only if

$$(p_1 - 1) \cdots (p_r - 1) \mid 3p_1 \cdots p_r.$$

Now note that if p is odd, then $p - 1$ is even. Therefore the left-hand side is divisible by at least $r - 1$ factors of 2, since only one of the primes can be 2. On the other hand, the right-hand side is divisible by at most 2 (at not 4) for the same reason. Therefore n can have at most one odd prime divisor, so either $n = 2^e$, $n = p^f$, or $n = 2^e p^f$ for some odd prime p and $e, f \geq 1$. In the first case, we have $\phi(2^e) = 2^{e-1} \mid 2^e$ indeed. In the second case, we have $\phi(p^f) = p^{f-1}(p-1) \nmid p^f$, since $p - 1$ is even but p^f is odd. In the last case, we have

$$(2-1)(p-1) = (p-1) \mid 3 \cdot 2 \cdot p.$$

Since $\gcd(p-1,p)=1$, this implies $p-1 \mid 6$, so $p=2,3,4,7$, hence $p=3,7$. Checking these, we conclude that $n=1$, $n=2^e$, $n=2^e3^f$, or $n=2^e7^f$ for $e,f\geq 1$.

Problem 5. We take $\log_3$ of both sides to get

$$\log_3(x^{40}) = 40\log_3 x \equiv \log_3 2 \pmod{78}.$$

Now $\log_3 2 = 4$ since $3^4 = 81 \equiv 2 \pmod{79}$. Therefore we solve

$$40\log_3 x \equiv 4 \pmod{78}.$$

Now $\gcd(40,78)=2 \mid 4$, so this becomes

$$20\log_3 x \equiv 2 \pmod{39}.$$

Note that $20^{-1} \equiv 2 \pmod{39}$, since $20\cdot 2 \equiv 1 \pmod{39}$, hence

$$\log_3 x \equiv 20^{-1}2 \equiv 4 \pmod{39}.$$

Therefore $\log_3 x = 4, 43$, and $x \equiv 3^4, 3^{43} \pmod{79}$. We compute that $3^4 \equiv 2 \pmod{79}$, and although it would be painful to compute $3^{43} \pmod{79}$, we notice that -2 is also a solution to the congruence, hence $3^{43} \equiv -2 \pmod{79}$.

For part (b), note that by (a) we have $2^{40} \equiv 2 \pmod{79}$, hence $2^{39} \equiv 1 \pmod{79}$, hence $o(2 \bmod 79) \mid 39$. Hence $o(2 \bmod 79) \neq 78$, so no, 2 is not a primitive root.

Problem 6. Let $N = p_1^{e_1}\cdots p_r^{e_r}$. Then

$$\sigma(N) = \frac{p_1^{e_1+1}-1}{p_1-1}\cdots\frac{p_r^{e_r+1}-1}{p_r-1} = 2N = 2p_1^{e_1}\cdots p_r^{e_r}.$$

Dividing both sides by $p_1^{e_1+1}\cdots p_r^{e_r+1}$ and multiplying by $(p_1-1)\cdots(p_r-1)$, we obtain

$$\frac{p_1^{e_1+1}-1}{p_1^{e_1+1}}\cdots\frac{p_r^{e_r+1}-1}{p_r^{e_r+1}} = 2\frac{p_1-1}{p_1}\cdots\frac{p_r-1}{p_r}$$

which rearranging becomes

$$\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right) = \frac{1}{2}\left(1-\frac{1}{p_1^{e_1+1}}\right)\cdots\left(1-\frac{1}{p_r^{e_r+1}}\right) < \frac{1}{2}.$$

Problem 7. We compute that $\phi(n) = 16\cdot 82 = 1312$ and using the extended Euclidean algorithm that $d \equiv e^{-1} \equiv 835^{-1} \equiv 11 \pmod{1312}$. Thus $P \equiv C^d \equiv 2^{11} \equiv 2048 \equiv 637 \pmod{1411}$ is her PIN number.

Problem 8. Note that if a has order h and b has order k modulo p, with $\gcd(h,k) = 1$, then ab has order hk modulo p. Together with the fact that -1 has order 2 modulo p, we conclude that

$$-53\cdot 39 \equiv 29 \pmod{131}$$

has order $2\cdot 5\cdot 13 = p-1$ modulo p, so $r = 29$ is a primitive root.

Problem 9. Consider the equation $x^2 \equiv a \pmod{p}$. Taking $\log_r$ of both sides, we obtain

$$2\log_r x \equiv \log_r a \pmod{p-1}.$$

This has a solution if and only if $\gcd(2,p-1) = 2 \mid \log_r a$, so a is a quadratic residue if and only if $\log_r a$ is even.

For (b), we write $a \equiv r^{\log_r a} \pmod{p}$. Now $r^u \bmod p$ is a primitive root if and only if $\gcd(u, p-1) = 1$. If a is quadratic residue, then $u = \log_r a$ is even, so $\gcd(u, p-1) = 2$, so a is not a primitive root.

For (c), all of the primitive roots modulo p are quadratic nonresidues by (a), so there are $\phi(\phi(p))$ such (of the $(p-1)/2$ quadratic nonresidues).

Problem 10. We apply Möbius inversion; since $\sigma_k(n)$ is the summatory function of $f(n) = n^k$, we conclude

$$\sum_{d|n} \mu(d)\sigma_k(n/d) = n^k.$$

For (b), we first note that $f(n) = n^k$ is (completely) multiplicative ($f(mn) = (mn)^k = m^k n^k = f(m)f(n)$). Therefore $\sigma_k(n)$ is multiplicative since it is the summatory function of f which is multiplicative. Now $\mu(n)\sigma_k(n)$ is multiplicative as well, since μ is multiplicative and hence

$$\mu(mn)\sigma_k(mn) = \mu(m)\mu(n)\sigma_k(m)\sigma_k(n) = (\mu(m)\sigma_k(m))(\mu(n)\sigma_k(n)),$$

if $\gcd(m, n) = 1$. Finally, $S_k(n)$ is the summatory function of $\mu(n)\sigma_k(n)$, so it is also multiplicative.

Thanks everyone, you were a great class. Good luck on the final!