MATH 255: ELEMENTARY NUMBER THEORY
EXAM #2

Problem 1.

(a) Find a root of the polynomial $x^5 + 10$ modulo 121.

Solution. We see that $1^5 + 10 \equiv 0 \pmod{11}$, so $x = 1$ is a root modulo 11. We use Hensel's lemma to find a root modulo $11^2 = 121$: if $f(x) = x^5 + 10$ then $f'(x) = 5x^4$; since $f'(1) = 5 \not\equiv 0 \pmod{11}$, we compute that $f'(1)^{-1} = 5^{-1} \equiv -2 \pmod{11}$, so a solution modulo 121 is given by

$$x \equiv 1 - f(1)/f'(1) \equiv 1 + 22 \equiv 23 \pmod{121}.$$

(b)* How many roots does $x^5 + 10$ have modulo $11^4 = 14641$?

Solution. By classwork, we know that $x^5 + 10 \equiv x^5 - 1 \pmod{11}$ has exactly 5 solutions, since $5 \mid \phi(11) = 11 - 1 = 10$. For each of these solutions, we have $f'(r) = 5r^4 \not\equiv 0 \pmod{11}$, else $r \equiv 0 \pmod{11}$ which is clearly impossible. Therefore, by Hensel's lemma, each of these lifts to a unique solution modulo 11^k for any $k \geq 2$. In particular, we find that there are exactly 5 solutions modulo 11^4.

Problem 2. (Short answer.)

(a) How many primitive roots are there modulo the prime 257?

Solution. There are $\phi(\phi(257)) = \phi(257 - 1) = \phi(256) = \phi(2^8) = 2^7 = 128$ primitive roots.

(b) Compute the Legendre symbol $\left(\dfrac{17}{47}\right)$.

Solution. We have $\left(\dfrac{17}{47}\right) = \left(\dfrac{47}{17}\right) = \left(\dfrac{13}{17}\right) = \left(\dfrac{17}{13}\right) = \left(\dfrac{4}{13}\right) = \left(\dfrac{2^2}{13}\right) = 1.$

(c) What are the last two decimal digits of 7^{642}?

Solution. We need to compute $7^{642} \pmod{100}$. Note that $\phi(100) = \phi(4)\phi(25) = 40$, and since $\gcd(7, 100) = 1$ we have $7^{40} \equiv 1 \pmod{100}$. Thus $7^{642} \equiv (7^{40})^{16} 7^2 \equiv 49 \pmod{100}$, so the last two digits are 49.

(d) Let f be a multiplicative function with $f(1) = 0$. Show that $f(n) = 0$ for all n.

Solution. We have $f(n) = f(1)f(n) = 0$, since $\gcd(1, n) = 1$ for all integers n.

(e) If a is a quadratic residue modulo p, show that a is not a primitive root modulo p.

Solution. Recall that a is a quadratic residue if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. In particular, the order of a divides $(p-1)/2$ so cannot be equal to $p - 1$.

Problem 3. Show that $a^6 - 1$ is divisible by 168 whenever $\gcd(a, 42) = 1$.

Solution. By the Chinese reminader theorem and the fact that $168 = 8 \cdot 3 \cdot 7$, it is enough to show this congruence holds modulo $8, 3, 7$. Modulo 8 and 3, we have $a^2 \equiv 1 \pmod{8}$ and $a^2 \equiv 1 \pmod{3}$ by inspection since $\gcd(a, 24) = 1$. Thus $a^6 \equiv (a^2)^3 \equiv 1 \pmod{24}$ as well. Modulo 7, we have $a^6 \equiv 1 \pmod{7}$ by Fermat's little theorem. The result follows.

Problem 4. Let n be a perfect number. Show that for all $k \in \mathbb{Z}_{\geq 2}$ that kn is abundant.

Solution. First suppose $\gcd(k, n) = 1$. Then $\sigma(kn) = \sigma(k)\sigma(n) = \sigma(k)(2n)$ since σ is multiplicative. But $\sigma(k) > k$ for all k (since it is the sum of divisors, and k is a divisor!), so $\sigma(kn) > k(2n) = 2nk$, so kn is abundant. If you got this far, that's good enough for me!

More generally, it is cleanest to consider the *abundance* function

$$h(m) = \frac{\sigma(m)}{m}.$$

We need to show that if $m \mid n$ then $h(m) \le h(n)$, with equality if and only if $m = n$. (Apply this with $n \mid kn$, and note that n is abundant if and only if $h(n) = 2$.) By definition, we have

$$h(n) = \sum_{d \mid n} \frac{d}{n}.$$

But if $d \mid n$, then $(n/d) \mid n$ and $(n/d)/n = 1/d$, so

$$h(n) = \sum_{d \mid n} \frac{1}{d}.$$

But then obviously

$$h(m) = \sum_{d \mid m} \frac{1}{d} \le \sum_{d \mid n} \frac{1}{d} = h(n)$$

if $m \mid n$ since every divisor of m is a divisor of n, and equality holds if and only if $m = n$.

Problem 5. The integer $n = pq = 280171$ is used in an RSA cryptosystem. Through espionage, you determine that

$$\sigma(n) = 281232.$$

Find p and q.

Solution. Since $n = pq$, we have $\sigma(n) = pq + p + q + 1$. Thus $\sigma(n) - n - 1 = p + q = 1060$. Therefore the polynomial

$$(x - p)(x - q) = x^2 - (p + q)x + pq = x^2 - 1060x + 280171$$

has p, q as roots. By the quadratic formula, we compute that $p, q = 530 \pm (1/2)\sqrt{1060^2 - 4(280171)} = 530 \pm 27 = 503, 557$.

Problem 6*. Let p be an odd prime and let r be a primitive root modulo p. Show that the order of $r + p$ modulo p^2 is either $p - 1$ or $p(p - 1)$.

Solution. Let k be the order of r modulo p^2, so that $r^k \equiv 1 \pmod{p^2}$ (and k is the smallest such positive integer). Then it follows that $r^k \equiv 1 \pmod{p}$ as well. But r is a primitive root, so we must have $(p - 1) \mid k$. On the other hand, by Euler's theorem we have $r^{\phi(p^2)} = r^{p(p-1)} \equiv 1 \pmod{p^2}$, so $k \mid p(p - 1)$. There is nowhere left to run: we must have $k = (p - 1), p(p - 1)$.