Problem Set 4
Solutions

Foundations of Number Theory

Math 435, Fall 2006

1. (10+10 pts.)

   (a) Let n be an integer. Then

   $$(n-4)^2 \equiv n^2 - 8n + 16 \equiv n^2 + 3n + 5 \mod 11.$$

   (b) By (a), $n^2 + 3n + 5$ is divisible by 11 precisely if $n \equiv 4 \mod 11$. If we set $n = 4 + 11k$ where $k \in \mathbb{Z}$, then

   $$n^2 + 3n + 5 \equiv 33 + 121k + 121k^2 \equiv 33 \not\equiv 0 \mod 121.$$

2. (20 pts.) For $n = 0$ we have $2^{2\cdot 0+1} \equiv 2 \equiv 9 \cdot 0^2 - 3 \cdot 0 + 2 \mod 54$. Now suppose we have already shown

   $$2^{2n+1} \equiv 9n^2 - 3n + 2 \mod 54$$

   for a certain $n \in \mathbb{N}$. Then

   $$2^{2(n+1)+1} \equiv 4 \cdot 2^{2n+1} \equiv 4 \cdot (9n^2 - 3n + 2) \mod 54.$$

   On the other hand

   $$9(n+1)^2 - 3(n+1) + 2 \equiv (9n^2 - 3n + 1) + (18n + 6) \mod 54,$$

   so we only need to show that

   $$3 \cdot (9n^2 - 3n + 2) \equiv 18n + 6 \mod 54.$$

   We have $3 \cdot (9n^2 - 3n + 2) = 27n^2 - 9n + 6$ and

   $$\begin{aligned} 27n^2 - 9n + 6 \equiv 18n + 6 \mod 54 &\iff 27n^2 - 27n \equiv 0 \mod 54 \\ &\iff 27n(n-1) \equiv 0 \mod 54, \end{aligned}$$

   and the last statement clearly holds since $2 | n(n-1)$.

3. (10+5+10+5 pts.)

   (a) For $x, y \in \mathbb{Z}$ and $i \in \mathbb{N}$ we have

   $$x^i - y^i = (x-y)(x^{i-1} + x^{i-2}y + \cdots + xy^{i-2} + y^{i-1}).$$

   In particular, taking $x = 10$ and $y = 4$, this shows that $x - y = 6$ divides $x^i - y^i = 10^i - 4^i$. By the Euler-Fermat Theorem we have $10^6 \equiv 1 \mod 7$, since $\phi(7) = 6$. This yields $10^{6k} \equiv 1^k \equiv 1 \mod 7$ for every $k \in \mathbb{N}$; in particular we get $10^{10^i - 4^i} \equiv 1 \mod 7$.

(b) By (a) we have

$$10^{10^i} \equiv 10^{4^i} \equiv 3^{4^i} \equiv (-4)^{4^i} \equiv 4^{4^i} \mod 7$$

for every $i \in \mathbb{N}$. (Since $10 \equiv 3 \equiv -4 \bmod 7$.)

(c) We show the claim by induction on $i \in \mathbb{N}$. For $i = 0$ have $4^{4^0} \equiv 4 \bmod 7$. Now suppose we have shown $4^{4^i} \equiv 4 \bmod 7$ for some $i \in \mathbb{N}$. Then

$$4^{4^{i+1}} \equiv \left(4^{4^i}\right)^4 \equiv 4^4 \equiv (4^2)^2 \equiv 2^2 \equiv 4 \mod 7$$

as required.

(d) By (b) and (c) we have

$$\sum_{i=1}^{10} 10^{10^i} \equiv \sum_{i=1}^{10} 4 \equiv 40 \equiv 5 \mod 7,$$

so the remainder is 5.

4. (20 pts.) We expect $\phi(22) = 10$ primitive roots modulo 23 (up to congruence mod 23). They are:

$$5, 7, 10, 11, 14, 15, 17, 19, 20, 21.$$

5. (10 pts.) Write $m = \prod_p p^{\alpha_p}$ and $n = \prod_p p^{\beta_p}$ (prime factorization of m and n). Then $m|n$ yields $\alpha_p \leq \beta_p$ for every p and thus

$$p^{\alpha_p - 1}(p-1) | p^{\beta_p - 1}(p-1) \qquad \text{if } p|m.$$

Hence

$$\phi(m) = \prod_{p|m} p^{\alpha_p - 1}(p-1)$$

divides

$$\phi(n) = \prod_{p|n} p^{\beta_p - 1}(p-1).$$

6. (20 pts. extra credit.) Let $n \in \mathbb{N}$. We note that $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, hence it is enough to show that $n^{13} \equiv n \bmod p$ for the primes $p = 2, 3, 5, 7, 13$. Now $\phi(p) = p - 1$ divides 12 for each such p! So if p does not divide n, then $n^{p-1} \equiv 1 \bmod p$ by Fermat's Little Theorem, hence $n^{12} \equiv 1 \bmod p$ since $(p-1)|12$, and thus $n^{13} \equiv n \bmod p$. If $p|n$, then clearly $n^{13} \equiv n \bmod p$.

Total: 100 pts. + 20 pts. extra credit.