MAT 311: Number Theory
Spring 2006

Solutions to HW5

1. (Davenport, pp.217, ex. 2.05) We would like to find the remainder when $x := (102^{73} + 55)^{37}$ is divided by $111 = 3 \cdot 37$. To do this, we first find the remainders $\mod 3$ and $\mod 37$; for then, those remainders will (uniquely) determine the remainder $\mod 111$ by Chinese remainder theorem (since 3 and 37 are coprime). Observe that $x^{37} \equiv x \mod 37$ by Fermat's little theorem; and $102^{73} = 102^{2\cdot 36} \cdot 102 \equiv 102 \equiv 18 \mod 37$. So $x \equiv 18 + 55 \equiv 9 \mod 37$. Similarly, $x^{37} \equiv x \mod 3$, again by FlT. Moreover, $102^{73} \equiv 0 \mod 3$ and $55 \equiv 1 \mod 3$. Hence $x \equiv 1 \mod 3$. So, the system

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 9 \mod 37 \end{aligned}$$

has a unique solution $\mod 111$ (by Chinese remainder theorem). It is straightforward to see that this solution is 46.

2. (Davenport, p.217, ex.2.07) We will find all natural numbers n for which $\varphi(n)$ is odd. Recall that if n has prime factorization $n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ (p_i are distinct primes)then $\varphi(n)$ can be computed as $\varphi(n) = \prod_{i=1}^{N} \left(p_i^{\alpha_i - 1}(p_i - 1) \right)$. Observe that if n has an *odd* prime divisor, say p_i then $p_i^{\alpha_i-1}(p_i - 1)$ is an even number; consequently, $\varphi(n)$ is even. On the other hand, n does not have an odd prime divisor, then $n = 2^N$ for some $N \geq 0$. In this case we have $\varphi(n) = 2^{N-1}(2-1) = 2^{N-1}$. So if $N \geq 2$ then $\varphi(n)$ is even. The remaining cases are $n = 2$ (when $N = 1$) and $n = 1$ (when $N = 0$). Obviously, $\varphi(1) = \varphi(2) = 1$. So, 1 and 2 are the only numbers whose φ-value is odd.

3. (Davenport, p.217, ex.2.12) Assume that p is an odd prime. We will show that $(p-2)! \equiv 1 \mod p$ and $(p-3)! \equiv (p-1)/2 \mod p$. To prove these we will use Wilson's theorem which says that $(p-1)! \equiv -1 \mod p$. Now, $(p-1)! = (p-1)(p-2)! \equiv (-1)(p-2)! \mod p = 1 \mod p$ where the last congruence follows from Wilson's theorem. Similarly, $1 \equiv (p-2)! = (p-2)(p-3)! \equiv (-2)(p-3)! \mod p$. So $2(p-3)! \equiv -1 \equiv p-1 \mod p$. But since $(2,p) = 1$ we can divide both side of this congruence by 2. This completes the proof.

4. We have already shown in the previous problems that $2(p-3)! \equiv -1 \mod p$ whenever p is an odd prime.

5. We aim to find the remainder of 5^{100} when divided by 7. In other words, we are trying to find $5^{100} \mod 7$. By Fermat's little theorem, $5^6 \equiv 1 \mod 7$. Hence $5^{100} = (5^6)^{14} \cdot 5^4 \equiv 5^4 = 625 \equiv 2 \mod 7$.

6. We want to find $18! \mod 437$. Since $437 = 19 \cdot 23$, we will first calculate the remainders $\mod 19$ and $\mod 23$. Indeed, $18! \equiv -1 \mod 19$ by Wilson's theorem (with $p = 19$). On the other hand, the same theorem tells us that $22! \equiv -1 \mod 23$, and so $22! = 22 \cdot 21 \cdot 20 \cdot 19 \cdot 19! \equiv (-1)(-2)(-3)(-4)18! = 24 \cdot 18! \equiv 18! \mod 23$. So, we have the system of congruences

$$\begin{aligned} 18! &\equiv -1 \mod 19 \\ 18! &\equiv -1 \mod 23. \end{aligned}$$

Hence, $18! \equiv -1 \mod [19, 23]$, *i.e.* $18! \equiv -1 \mod 437$. So the remainder is $437 - 1 = 436$.

7. We want to determine the last digit of 7^{1000}. Equivalently, we would like to find $7^{1000} \mod 10$. By Euler's theorem $7^{\varphi(10)} = 7^4 \equiv 1 \mod 10$ since $(7, 10) = 1$. So, $7^{1000} = (7^4)^{250} \equiv 1^{250} \equiv 1 \mod 10$. So, the remainder is 1.

8. We aim to find the last digit of 3^{100} in its base 7 expansion. Equivalently, we would like to determine $3^{100} \mod 7$. By Fermat's little theorem $3^6 \equiv 1 \mod 7$; hence $3^{100} = (3^6)^{14} \cdot 3^4 \equiv 3^4 \equiv 81 \equiv 4 \mod 7$.

9. We will show that $42 \mid (n^7 - n)$ for all positive n. Since $42 = 2 \cdot 3 \cdot 7$, it suffices to show that each of these primes indeed divide $n^7 - n$. In other words, we need to show that $n^7 \equiv n \mod 2, 3, 7$. All of these congruences follow from Fermat's little theorem, as

$$\begin{array}{llll} n^2 \equiv n & \mod 2 & \Rightarrow & n^7 = (n^2)^3 \cdot n \equiv n \mod 2 \\ n^3 \equiv n & \mod 3 & \Rightarrow & n^7 = (n^3)^2 \cdot n \equiv n \mod 3 \\ n^7 \equiv n & \mod 7. & & \end{array}$$

10. We will prove that $\varphi(n)\varphi(m) = \varphi((n,m))\,\varphi([n,m])$. First observe that we can rearrange the order of prime powers in the prime factorization of n and m so that we can write $n = p_1^{\alpha_1} \dots p_K^{\alpha_K} p_{K+1}^{\alpha_{K+1}} \dots p_{N+1}^{\alpha_{N+1}}$ and $n = p_1^{\beta_1} \dots p_K^{\beta_K} q_{K+1}^{\beta_{K+1}} \dots q_{M+1}^{\beta_{M+1}}$ where $\alpha_i, \beta_i > 0$, N, M some natural numbers (0 if n or m is 1), and K some nonnegative integer (0 if n and m does not have a common prime factor). Now, clearly

$$\begin{aligned} (n,m) &= \prod_{i=1}^{K} p_i^{\min\{\alpha_i,\beta_i\}} \\ [n,m] &= \left(\prod_{i=1}^{K} p_i^{\max\{\alpha_i,\beta_i\}}\right) \cdot \left(\prod_{i=K+1}^{N} p_i^{\alpha_i}\right) \cdot \left(\prod_{i=K+1}^{M} q_i^{\beta_i}\right). \end{aligned}$$

By the formula to compute φ-function given in Problem 2, we have

$$\varphi(n)\varphi(m) = \left(\prod_{i=1}^{K} p_i^{(\alpha_i-1)+(\beta_i-1)}(p_i-1)^2\right) \cdot \left(\prod_{i=K+1}^{N} p_i^{\alpha_i-1}(p_i-1)\right) \cdot \left(\prod_{i=K+1}^{M} q_i^{\beta_i-1}(q_i-1)\right)$$

and

$$\begin{aligned} \varphi((n,m))\,\varphi([n,m]) &= \left(\prod_{i=1}^{K} p_i^{(\min\{\alpha_i,\beta_i\}-1)+(\max\{\alpha_i,\beta_i\}-1)}(p-1)^2\right) \cdot \\ &\quad \cdot \left(\prod_{i=K+1}^{N} p_i^{\alpha_i-1}(p_i-1)\right) \cdot \left(\prod_{i=K+1}^{M} q_i^{\beta_i-1}(q_i-1)\right). \end{aligned}$$

Clearly the above two expressions are the same since $\min\{\alpha_i, \beta_i\} + \max\{\alpha_i, \beta_i\} = \alpha_i + \beta_i$.

11. Let $\tau(n)$ denote the number of positive divisors of n. It is known that τ is a multiplicative function, that is, $\tau(mn) = \tau(m) \cdot \tau(n)$ **if** $(n,m) = 1$. If $n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ is the prime factorization of n, then

$$\tau(n) = (\alpha_1 + 1) \dots (\alpha_N + 1). \qquad (*)$$

If $\tau(n) = 3$, then 3 is a product of the form (*). Since all the factors $(\alpha_i + 1)$ are ≥ 2 this is possible only when $N = 1$ and $\alpha_1 = 2$. The smallest such n is obviously 4 (by taking $p_1 = 2$. Of course we could find this n by trial and error, but solving the problem like this gives an idea about how to solve similar problems: Let's find the smallest n with $\tau(n) = 13 \cdot 31$. Then $13 \cdot$ 31 of the form (*); so again the only possibilities for this is that (1) $N = 2$ and $\alpha_1 = 12$ and $\alpha_2 = 31$ or (2) $N = 1$ and $\alpha_1 = 13 \cdot 31 - 1$. If we want to get smaller n's, we should choose smaller exponents; thus, we should consider the first case. So, n must be of the form $n = p_1^{\alpha_1} p_2^{\alpha_2}$ for some distinct primes p_1, p_2. The two smallest primes are 2 and 3. To minimize n, 3 must have smaller exponent. Hence $n = 2^{30} \cdot 3^{12}$.

12. We aim to find all positive integers with $\tau(n) = 4$. Again, 4 should be written in the form of (*). This is only possible when
(Case 1) $N = 2$ and $\alpha_1 = 1$, $\alpha_2 = 1$ (corresponding to the factorization $4 = 2 \cdot 2$),
or
(Case 2) $N = 1$ and $\alpha_1 = 3$ (corresponding to the trivial factorization $4 = 1 \cdot 4$).
In the first case, n is of the form $n = p^a \cdot q^b$ (here, p, q are distinct primes), and in the second of the form $n = p^3$ (where p is prime).