IX. Number Theory

Po-Shen Loh

June 30, 2003

1 Warm-Ups

1. (Po's Lemming #2) Prove that there are infinitely many non-primes.
2. Suppose that $(a, m) = 1$. Prove that $ab \equiv ac \pmod{m} \Rightarrow b \equiv c \pmod{m}$.
3. Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial with integer coefficients. Show that if r consecutive values of f (i.e. values for consecutive integers) are all divisible by r, then $r | f(m)$ for all $m \in \mathbb{Z}$.

   Solution: Just plug in $k + r$ and you get the same residue (mod r) as if you plugged in k.

2 Theorems

1. Let a, n, m be positive integers with $a \geq 2$ and $n \geq m$. Prove that

$$(a^n - 1, a^m - 1) = (a^{(n,m)} - 1).$$

   Solution: Use the Euclidean algorithm with the identity:

$$a^n - 1 = (a^m - 1)(a^{n-m} + \cdots + a^{n-km}) + a^{n-km} - 1$$

2. (Euler's Theorem). If $(a, m) = 1$, then:

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

   Solution: Draw out complete residue set $a_1, a_2, \ldots, a_k$, where $k = \phi(m)$. Now $aa_1, aa_2, \ldots, aa_k$ is also a complete residue set by cancellation, so their total products are congruent modulo m. Yet we can cancel out the common factor of $a_1 a_2 \cdots a_k$ because that is relatively prime to m. And we are done.

3. If $(a, m) = 1$, then $\text{ord}_m a | \phi(m)$.

   Solution: Use the first Theorem to show:

$$m | (a^{\phi(m)} - 1, a^{\text{ord}} - 1) = a^{(\phi(m), \text{ord})} - 1$$

   so $(\phi(m), \text{ord}_m a) = \text{ord}_m a$ which gives us what we want.

4. (Partial Converse of Fermat's Little Theorem). If there is an a for which $a^{m-1} \equiv 1 \pmod{m}$, while none of the congruences $a^{(m-1)/p} \equiv 1 \pmod{m}$ hold, where p runs over the prime divisors of $m - 1$, then m is prime.

   Solution: By def of ord, we get that $\text{ord}_m a | m - 1$ but it doesn't divide any factors of it; therefore, $\text{ord}_m a = m - 1$. But since $\text{ord}_m a | \phi(m)$ and $\phi(m) \leq m - 1$, we must have precisely that $\phi(m) = m - 1$ so m has no divisors other than 1 or itself, and is prime.

5. (Dirichlet). If $(a, d) = 1$, then the arithmetic progression $\{a, a+d, a+2d, \ldots\}$ contains infinitely many primes.

6. (Chinese Remainder Theorem). If $\{m_k\}$ are pairwise relatively prime, then the solution to the system:

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\vdots \\ x &\equiv r_n \pmod{m_n} \end{aligned}$$

is precisely one of the residue classes modulo $m_1 m_2 \cdots m_n$.

Solution: Induction on n. Do it for a pair; suffices to show that there is precisely one solution in $\{1, 2, \ldots, m_2 m_1\}$. Since $(m_1, m_2) = 1$, the sequence $(m_1, 2m_1, \ldots, m_2 m_1)$ is a permutation of the residues modulo m_2. Hence translating each of them by $+a_1$, these still uniquely cover the residue classes. Now they also repeat at $(m_2 + 1)m_1$, so we get a_2 exactly once every $m_2 m_1$.

3 Problems

1. (MOP98/1/1). Prove that the sum of the squares of 3, 4, 5, or 6 consecutive integers is not a perfect square.

   Solution: 3: go mod 3; 4, 5, 6: go mod 4

2. (Czech-Slovak97/5). Several integers are given (some of them may be equal) whose sum is equal to 1492. Decide whether the sum of their seventh powers can equal 1998.

   Solution: Fermat's little theorem: $x^7 \equiv x \pmod{7}$.

3. (MOP97/2/4). Show that 19^{19} cannot be written as $m^3 + n^4$, where m and n are positive integers.

   Solution: go mod 13

4. (Russia97/28). Do there exist real numbers b and c such that each of the equations $x^2 + bx + c = 0$ and $2x^2 + (b+1)x + c + 1 = 0$ have two integer roots?

   Solution: No. Suppose they exist. Then $b + 1$ and $c + 1$ are even integers (since $-(b+1)/2$ is the sum of roots of 2nd equation, and $(c+1)/2$ is product of roots), so b and c are odd and $b^2 - 4c \equiv 5 \pmod{8}$, since c is odd, and that cannot be a perfect square.

5. Prove that $x^2 + y^2 + z^2 = 7w^2$ has no solutions in integers.

   Solution: Assume on the contrary that (x, y, z, w) is a nonzero solution with $|w| + |x| + |y| + |z|$ minimal. Modulo 4, we have $x^2 + y^2 + z^2 \equiv 7w^2$, but every perfect square is congruent to 0 or 1 modulo 4. Thus we must have x, y, z, w even, and $(x/2, y/2, z/2, w/2)$ is a smaller solution, contradiction.

6. (MOP97/6/1). Four integers are marked on a regular heptagon. On each step we simultaneously replace each number by the difference between this number and the next number on the circle (that is, the numbers a, b, c, d are replaced by $a - b$, $b - c$, $c - d$, and $d - a$). Is it possible after 1996 such steps to have numbers a, b, c, d such that the numbers $|bc - ad|, |ac - bd|, |ab - cd|$ are all primes?

   Solution: After 4 steps, all even, so then get them all to be multiples of 4, not prime.

7. (USAMO98/1). The sets $\{a_1, a_2, \ldots, a_{999}\}$ and $\{b_1, b_2, \ldots, b_{999}\}$ together contain all the integers from 1 to 1998. For each i, $|a_i - b_i| = 1$ or 6. For example, we might have $a_1 = 18$, $a_2 = 1$, $b_1 = 17$, $b_2 = 7$. Show that $\sum_{i=1}^{999} |a_i - b_i| = 9 \pmod{10}$.

   Solution: If $|a_i - b_i| = 6$, then a_i and b_i have the same parity, so the set of such a_i and b_i contains an even number of odd numbers. But if $|a_i - b_i| = 1$, then a_i and b_i have opposite parity, so each such pair includes just one odd number. Hence if the number of such pairs is even, then the set of all such a_i and b_i also has an even number of odd numbers. But the total number of a_i and b_i which are odd is 999 which is odd. Hence the number of pairs with $|a_i - b_i| = 1$ must be odd, and hence the number of pairs with $|a_i - b_i| = 6$ must be even. Suppose it is $2k$. Then $\sum |a_i - b_i| = (999 - 2k)1 + 2k6 = 999 + 10k \equiv 9 \pmod{10}$.

8. (StP96/22). Prove that there are no positive integers a and b such that for each pair p, q of distinct primes greater than 1000, the number $ap + bq$ is also prime.

   Solution: Suppose a, b are so chosen, and let m be a prime greater than $a+b$. By Dirichlet's theorem, there exist infinitely many primes in any nonzero residue class modulo m; in particular, there exists a pair p, q such that $p \equiv b \pmod{m}, q \equiv -a \pmod{m}$, giving $ap + bq$ divisible by m, a contradiction.

9. (Czech-Slovak97/4). Show that there exists an increasing sequence $\{a_n\}_1^\infty$ of natural numbers such that for any $k \geq 0$, the sequence $\{k + a_n\}$ contains only finitely many primes.

   Solution: Let p_k be the k-th prime number, $k \geq 1$. Set $a_1 = 2$. For $n \geq 1$, let a_{n+1} be the least integer greater than a_n that is congruent to $-k$ modulo p_{k+1} for all $k \leq n$. Such an integer exists by the Chinese Remainder Theorem. Thus, for all $k \geq 0$, $k + a_n \equiv 0 \pmod{p_{k+1}}$ for $n \geq k+1$. Then at most $k+1$ values in the sequence $\{k + a_n\}$ can be prime; from the $k+2$-th term onward, the values are nontrivial multiples of p_{k+1} and must be composite.

10. (Russia96/20). Do there exist three natural numbers greater than 1, such that the square of each, minus one, is divisible by each of the others?

    Solution: Such integers do not exist. Suppose $a \geq b \geq c$ satisfy the desired condition. Since $a^2 - 1$ is divisible by b, the numbers a and b are relatively prime. Hence the number $c^2 - 1$, which is divisible by a and b, must be a multiple of ab, so in particular $c^2 - 1 \geq ab$. But $a \geq c$ and $b \geq c$, so $ab \geq c^2$, contradiction.

11. (Japan96/2). Let m and n be positive integers with $\gcd(m, n) = 1$. Compute $\gcd(5m + 7m, 5n + 7n)$.

    Solution: Let $s_n = 5^n + 7^n$. If $n \geq 2m$, note that $s_n = s_m s_{n-m} - 5^m 7^m s_{n-2m}$, so $\gcd(s_m, s_n) = \gcd(s_m, s_{n-2m})$. Similarly, if $m < n < 2m$, we have $\gcd(s_m, s_n) = \gcd(s_m, s_{2m-n})$. Thus by the Euclidean algorithm, we conclude that if $m + n$ is even, then $\gcd(s_m, s_n) = \gcd(s_1, s_1) = 12$, and if $m + n$ is odd, then $\gcd(s_m, s_n) = \gcd(s_0, s_1) = 2$.

12. (MOP97/5/4). Find all positive integers n such that $2^{n-1} \equiv -1 \pmod{n}$.