Number Theory

Math 341, Spring 2010

Professor Ben Richert

Take home Final

Due: Monday, June 7, by 4pm
in Dr. Richert's office, bld. 25, room 325
or (if the baby interferes),
in the department office, bld. 25, room 208

This exam is to be completed on your own. The only resources you may use are your textbook, class notes, your returned homework, and a calculator; on problem number 3 you may use a computer algebra system such as *Mathematica* (but it is not required or necessary that you do so). You may not use the internet, or consult each other.

Problem 1 (10pts) Compute the last digit of 3^{213}.
Problem 2 (10pts) Evaluate the Legendre symbol (3658/12703).
Problem 3 (10pts) Give all solutions (modulo 1216) to the system:

$$\begin{aligned} 11x + 16y &\equiv 103 \pmod{1216} \\ 3x + 19y &\equiv 205 \pmod{1216} \end{aligned}$$

Problem 4 (10pts) If $a \mid bc$, prove that $a \mid (a,b)(a,c)$.
Problem 5 (15pts) Let n be an integer, and consider the 10 consecutive numbers $\{n, n+1, n+2, \dots, n+9\}$. Suppose that none of these is divisible by 11.

(a–5pts) Prove that these 10 numbers are incongruent modulo 11.
(b–5pts) Prove that $\{n, n+1, n+2, \dots, n+9\} \equiv \{1, \dots, 10\} \pmod{11}$.
(c–5pts) Prove that $n(n+1)\cdots(n+9) \equiv -1 \pmod{11}$.

Problem 6 (10pts) Suppose that p is an odd prime such that $p \equiv 1 \pmod 4$ and r is a primitive root of p. Prove that $-r$ is also primitive.
Problem 7 (10pts) Let p be an odd prime and $a \in \mathbb{N}$ be such that $(a,p) = 1$. Define the *size* of a modulo p to be the minimum natural number t (nonzero) such that for some $i \in \mathbb{N} \cup \{0\}$ we have $a^{i+t} = a^i$. Prove that the size of a modulo p is equal to the order of a modulo p.
Problem 8 (10pts) Prove the following theorem: Let p and q be distinct odd primes and $N = pq$. Then N has no primitive roots. (Hint: for r relatively prime to N, consider r^d modulo N for $d = \dfrac{(p-1)(q-1)}{2}$).
Problem 9 (10pts) Consider an odd prime $p \neq 5$ and note that

$$(5/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

This is not difficult to demonstrate—you may assume it for this problem. Prove that there are infinitely many primes of the form $5k \pm 1$. (Hint: if not, consider $N = (2p_1 \cdots p_r \cdot q_1 \cdots q_s)^2 - 5$ where $p_1, \dots, p_r$ are the the finitely many primes of the form $5k+1$, and $q_1, \dots, q_s$ are the finitely many primes of the form $5k-1$).

Problem 10 (20pts) Let $a, b \in \mathbb{N}_{>1}$ be relatively prime and let $\{a_i\}_{i\in\mathbb{N}}$ be the sequence defined recursively as

$$\begin{aligned} a_1 &= a \\ a_2 &= a_1 + b \\ a_3 &= a_1 a_2 + b \\ &\vdots \\ a_i &= a_1 \cdots a_{i-1} + b \\ &\vdots \end{aligned}$$

(a–10pts) Show that the elements of the sequence $\{a_i\}$ are pairwise relatively prime (meaning, $(a_i, a_j) = 1$ for all $i \neq j$). Hint: suppose not, let i be the smallest index such that there is $j > i$ with $(a_i, a_j) \neq 1$, choose a prime p dividing a_i and a_j, and use the definition of a_j to argue that $p \mid b$. What does this imply if $i = 1$? If $i > 1$, what does the equation for a_i tell you (remember, a_i is supposed to be minimal)?

(b–10pts) Use part (a) to conclude that there are infinitely many primes (thus giving an alternative to Euclid's proof).

Problem 11 (10pts) Let $n = 2m$ where m is an odd natural number. Prove that $\sum_{d \mid n} (-1)^{n/d}\phi(d) = 0$. (Hint: recall that for an odd natural t, $\phi(2t) = \phi(2)\phi(t) = \phi(t)$).