115A Midterm

Monday November 8, 2004

ANSWER EACH QUESTION ON A SEPARATE SHEET OF PAPER

Name Eratosthenes

Signature E2

Pens, pencils and erasers are the only tools allowed in this exam

Question 1 Warmup:

(i) Find all integers n where $n \equiv 1 \bmod 31$.

(ii) Let $m \in \mathbb{N}$. List two different complete sets of residues mod m.

(iii) Compute $(21, 56)$ using the extended Euclidean algorithm. Show your steps and also express your answer as a linear combination of 21 and 56.

(iv) What is a Mersenne prime?

Question 2 Let positive integers m_1, m_2, m_3 be pairwise relatively prime. Now suppose ν_1, ν_2 and ν_3 are inverses of m_2m_3, m_3m_1 and m_1m_2 modulo m_1, m_2 and m_3, respectively. Prove that

$$x = a_1\nu_1m_2m_3 + a_2\nu_2m_3m_1 + a_3\nu_3m_1m_2$$

is the unique solution modulo $m_1m_2m_3$ of the system of linear congruences

$$x \equiv a_1 \bmod m_1\,, \qquad x \equiv a_2 \bmod m_2\,, \qquad x \equiv a_3 \bmod m_3\,.$$

Question 3 Let $k \in \mathbb{N}$. Show there are infinitely many primes $6k + 5$.

Question 4 Find 1001 consecutive composite integers.

Question 5 Show that every positive integer is the product of possibly a square and a "square-free" integer (no factor other than 1 appears more than once).

Question 6 What is your favorite number?

Q1 (i) $n = 1 + 31k = \{\ldots, -30, 1, 32, \ldots\}$ $\quad k \in \mathbb{Z}$

(ii) $\{0, 1, \ldots, m-1\}$

or $\{1, \ldots, m\}$

(iii) $56 = 2 \cdot 21 + 14 \Leftrightarrow 14 = 1 \cdot 56 - 2 \cdot 21$

$21 = 1 \cdot 14 + 7 \Leftrightarrow 7 = 1 \cdot 21 - 1 \cdot 14$

$= 1 \cdot 21 - 1 \cdot (1 \cdot 56 - 2 \cdot 21)$

$= -1 \cdot 56 + 3 \cdot 21$

$14 = 2 \cdot 7 + 0 \leftarrow$ terminates

$(56, 21) = 7 = -1 \cdot 56 + 3 \cdot 21$

(iv) A Mersenne prime takes the form $2^n - 1 \quad n \in \mathbb{N}$

Q2 x is a solution because

$$a_2 \nu_2 m_3 m_1 + a_3 \nu_3 m_1 m_2 \equiv 0 \mod m_1$$

and $a_1 \equiv a_1 \nu_1 m_2 m_3 \mod m_1$, since

$$\nu_1 m_2 m_3 \equiv 1 \mod m_1$$

$\Rightarrow x \equiv a_1 \mod m_1$, similarly for the other two congruences.

To prove uniqueness suppose x and x_1 are both solutions then

$$x \equiv x_1 \equiv a_1 \mod m_1 \Rightarrow m_1 \mid x - x_1 \quad \text{---- (1)}$$

$$x \equiv x_2 \equiv a_2 \mod m_2 \Rightarrow m_2 \mid x - x_1 \quad \text{---- (2)}$$

$$x \equiv x_3 \equiv a_3 \mod m_3 \Rightarrow m_3 \mid x - x_1 \quad \text{---- (3)}$$

(1) says $x - x_1 = b_1 m_1$

(2) says $x - x_1 = b_2 m_2 m_1$ because $m_2 \nmid m_1$

(3) says $x - x_1 = b_3 m_3 m_2 m_1$ because $m_3 \nmid m_1, m_2$

$\Rightarrow m_1 m_2 m_3 \mid x - x_1$

$\Rightarrow x - x_1 \equiv 0 \mod m_1 m_2 m_3$

$\Rightarrow x \equiv x_1 \mod m_1 m_2 m_3$ QED.

Q3 By contradiction, suppose there are finitely many such primes $p_1, p_2, \dots p_r$.

Consider $q = 6p_1p_2\cdots p_r + 5$ which must be composite.

But all primes, save 2 & q, take the form

$$6k+1 \quad \text{or} \quad 6k+5.$$

Let $p_i \nmid q$ $(1 \le i \le r)$ so the prime divisors of q take the form $6k+1$.

Noting that

$$(6k+1)(6k'+1) = 6(6kk'+k+k') + 1$$

we see that q must take the form $6l+1$ $\lightning$

QED

Q4 $1002! + 2, 1002! + 3, \ldots, 1002! + 1002$

because $1002! = 2 \cdot 3 \cdot \ldots \cdot 1002$ has $2, 3, \ldots, 1002$ as factors.

Q5 By fundamental theorem of arithmetic, any positive integer is (uniquely) a product of powers of primes.

If a given prime p appears an even number of times p^{2n} we have $p^{2n} = (p^n)^2$ a square

Alternatively for an odd power $p^{2n+1} = (p^n)^2 \cdot p$, a product of a square and a square-free integer.

This property is not violated by taking a product over all prime powers appearing in a given integer. QED