

**MATH. 104A, FINAL (6/12/06)**

You have **3 hours** for this exam. There are 6 questions. Please write legibly. **No calculators are allowed.**

**(1a)** (15 points) Suppose that apples cost 15 cents each, while oranges cost 40 cents each. Mary has a 5 dollar note and wants to spend it all on apples and oranges. If she wants the number of apples and oranges she buys to be as equal as possible, how many apples and oranges can she buy?

**(2a)** (5 points) Give Euclid's proof that there are infinitely many prime numbers.

(b) (5 points) Let  $p_n$  be the  $n$ -th prime (so  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$  and so on). Using (a) and mathematical induction, show that

$$p_n \leq 2^{2^{n-1}}.$$

(c) (5 points) Show that there are infinitely many prime numbers of the form  $3k + 2$ .

**(3a)** (5 points) Let  $p$  be a prime and let  $a$  be an integer not divisible by  $p$ . What does it mean to say that  $a$  is a quadratic residue mod  $p$ ? Give the definition of the Legendre symbol  $\left(\frac{a}{p}\right)$ .

(b) (10 points) For which primes  $p > 3$  does the quadratic congruence  $x^2 \equiv -6 \pmod{p}$  have solutions?

(c) (5 points) Find all solutions of  $x^2 - 6x + 14 \equiv 0 \pmod{149}$ .

(4) (15 points) A group of 10 pirates has just acquired a chest of gold coins. From their experience with these things, they could tell that there are at least 900 coins but not more than 1200 coins. When they tried to divide the coins evenly among themselves, they found that there is 1 extra coin left over. Naturally, a fight broke out for this last coin, with the tragic result that one of the pirates was killed.

The remaining pirates tried to redistribute the coins evenly among themselves and this time, there are two extra coins. As to be expected, a fight broke out with the result that 2 pirates lost their lives. This time, however, the remaining pirates were able to divide the coins evenly among them. How many coins were there?

**(5a)** (5 points) Let  $a$  and  $n$  be relatively prime. Show that if  $a^k \equiv 1 \pmod{n}$ , then the order of  $a \pmod{n}$  divides  $k$ .

(b) (5 points) Deduce from (a) that the order of  $a \pmod{n}$  divides  $\phi(n)$  (where  $\phi$  is Euler's  $\phi$ -function). If you use a theorem from class, state that theorem clearly.

(c) (5 points) Find a primitive root mod 83.

(6) Decide if the following are true or false. Justify your answers. Each part is worth 4 points.

(a) If  $GCD(a, b, c) = 1$ , then  $a, b, c$  are pairwise relatively prime.

(b) If  $f$  and  $g$  are two multiplicative functions, then the function  $f + g$ , defined by  $(f + g)(x) = f(x) + g(x)$ , is also multiplicative.

(c) If  $a$  is a primitive root mod  $n$ , then the modular inverse of  $a$  is also a primitive root mod  $n$ .

(d) There are no integer solutions to the equation  $x^2 - 5y^2 = 17$ .

(e) If  $p$  is an odd prime, one can find integers  $x$  and  $y$  satisfying  $x^2 + y^2 \equiv -1 \pmod{p}$ .