

This is a closed-book exam: no notes, books or calculators are allowed. Explain your answers as clearly and as completely as you possibly can. The blue book that you hand in at the end of the exam is your only representative when the exam is graded.

- 1** (4 points). Find an integer  $x$  such that  $x \equiv 7 \pmod{37}$  and  $x^2 \equiv 12 \pmod{37^2}$ .
- 2** (5 points). Let  $n$  be an odd positive integer. Show that  $n$  is a perfect square if and only if  $\left(\frac{b}{n}\right) = 1$  for all integers  $b$  prime to  $n$ .
- 3** (5 points). Express the infinite continued fraction  $\overline{[1, 2, 3]}$  in the form  $\frac{a + \sqrt{b}}{c}$  with  $a, b$  and  $c$  integers.
- 4** (6 points). Find a positive integer  $f$  so that  $x^{271f} \equiv x \pmod{29 \cdot 31}$  for all  $x$  prime to  $29 \cdot 31$ .
- 5** (4 points). Decide whether or not 263 is a square mod 331. (Both numbers are primes.)
- 6** (5 points). Use the equations

$$3469 = 2 \cdot 1298 + 873$$

$$1298 = 1 \cdot 873 + 425$$

$$873 = 2 \cdot 425 + 23$$

$$425 = 18 \cdot 23 + 11$$

to write  $3469/1298$  as a simple continued fraction.

- 7** (6 points). Let  $p$  be a prime that is congruent to 1 mod 4. View the quadratic residues (i.e., squares) mod  $p$  as integers between 0 and  $p - 1$ . Show that the sum of these integers is  $p\left(\frac{p-1}{4}\right)$ . [Example: when  $p$  is 5, the residues are 1 and 4. Their sum is 5.]

- 8** (4 points). If eggs in a basket are taken out 2, 3, 4, 5 and 6 at a time, there are 1, 2, 3, 4 and 5 eggs left over, respectively. If they are taken out 7 at a time, there are no eggs left over. What is the least number of eggs that can be in the basket?

- 9** (5 points). Show that a positive integer  $n$  is a perfect number if and only if  $\sum_{d|n} \frac{1}{d} = 2$ .

If  $n$  is a perfect number, show that  $tn$  is not a perfect number when  $t > 1$ .

- 10** (6 points). Let  $n$  be a positive integer. Suppose that the Fermat number  $p = 2^{2^n} + 1$  is prime. Prove that  $3^{(p-1)/2} \equiv -1 \pmod{p}$ .