

18.781: FINAL EXAM

MAY 23, 2003

Instructions: To receive credit for a solution, your answer must be explained fully in complete sentences. Correct answers without proper explanation will receive no credit.

No notes, books, or calculators are allowed.

Each question is worth ten (10) points, and the questions are arranged in no particular order.

1. (a) Show that $3^{20} \equiv 1 \pmod{100}$.
(b) Use (a) to compute the last two digits in the ordinary decimal representation of 3^{400} .

2. State and prove the Chinese remainder theorem.

- 3.** (a) Compute the value of the infinite periodic continued fraction $\langle 9, \overline{9, 18} \rangle$.
- (b) Does $X^2 - 83Y^2 = -1$ have a non-trivial solution? How about $X^2 - 83Y^2 = 1$?

4. Let a, b, c be integers and p a prime not dividing a . Prove that the number of solutions to the equation

$$aX^2 + bX + c \equiv 0 \pmod{p}$$

is given by $1 + \left(\frac{D}{p}\right)$ where $D = b^2 - 4ac$.

5. (a) Define what is meant by the *order* of an integer a modulo another integer m for which $(a, m) = 1$.

(b) Suppose p is a prime equal to $2^{2^n} + 1$ for some positive integer n . Show that

$$3^{(p-1)/2} \equiv -1 \pmod{p}.$$

(c) With p as in (b), compute the order of 3 modulo p .

6. (a) Prove that the congruence

$$(X^2 - 2)(X^2 - 17)(X^2 - 34) \equiv 0 \pmod{p}$$

has a solution for every prime p .

(b) For which primes p is 34 a square modulo p ?

7. Compute $E(\mathbb{Q})_{\text{tors}}$ for the elliptic curve E given by the equation $Y^2 = X^3 + 1$ (the formula $D = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$ may be helpful).

8. (a) Show that the curve C given by the equation $X^4Y^4 - 1$ has infinitely many rational points (hint: This requires no theory).

(b) State Falting's theorem (also known as the Mordell conjecture). Explain why (a) does not give a contradiction.