# Problem set 14: fermat’s little theorem

1. *Review:* Prove that gcd(a, b) = gcd(a – kb, b) for any integer, k.
2. Review: Let a and b be integers, not both 0. Prove that there exist integers x and y such that ax + by = gcd(a, b).
3. Find integers x and y such that ax + by = gcd(7777, 3234).
4. Let a and b be integers, not both 0. Prove that

{ax + bx| a, b Z, ax + by >0} = {k gcd{a, b}| k Z}

1. Does the Diophantine equation 77721x + 17078y = 4 have a solution? If so, find one; if not, explain why.
2. Give Euclid’s proof that there exist infinitely many primes.

(a) $\sqrt{3} $is irrational

(b) $1-7\sqrt{3}$ is irrational

(c) $\sqrt{2}+\sqrt{3}$ is irrational

1. State the Fundamental Theorem of Arithmetic.
2. Prove that a and b are relatively prime if and only if there exist integers x, y for which

ax + by = 1.

1. Euclid’s lemma: Prove that if q divides ab and q is prime then either q divides a or

q divides b.

Is this statement still true if one removes the hypothesis that q be prime?

What if one assumes that gcd(b, q) = 1 ?

1. Prove the following division rule for modular arithmetic: If ca cb (mod n) and

gcd(c, n) = 1, then a b (mod n).

1. More generally, prove that if ca cb (mod n) then a b (mod n/d), where

d = gcd(a, b).

1. State and prove Fermat’s little theorem.
2. Using Fermat’s theorem show that 17 is a divisor of 11104 + 1.
3. Using Fermat’s little theorem, compute 331 (mod 7), 2925 (mod 11), and

128129 (mod 17).

1. Let k = 20082 + 22008. What is the units digit of k2 + 2k ? (hint: think mod 10)

(a) 0 (b) 2 (c) 4 (d) 6 (e) 8

1. Find 220 + 330 + 440 + 550 + 660 (mod 7)

Supplement:

(from Art of Problem Solving)

We are particularly interested in Proof 2 (Inverses).





 



