# Problem set 13: extended GCD, fermat’s little theorem

* 1. Let a and b be integers, not both 0. Define gcd(a, b).
	2. Find gcd(2584, 1597)
	3. Prove that gcd(a, b) = gcd(a – kb, b) for any integer, k.
	4. Using the extended Euclidean algorithm, find integers x and y such

that ax + by = gcd(a, b) when:

1. a = 34, b = 459
2. a = 272, b =4356
3. a = 156 b = 572
	1. Using the extended Euclidean algorithm, find integers x and y such that 3789406027x + 18272779829y = gcd(37894060279, 18272779829). Of course, the calculation below is of great help.



1. State the well-ordering principle.
2. State and prove the division algorithm.
3. Let a and b be integers, not both 0. Prove that there exist integers x and y such that ax + by = gcd(a, b)

.

1. Give Euclid’s proof that there exist infinitely many primes.
2. $ Prove Pythagoras'$ theorem$ that \sqrt{2}$ is irrational.
3. Prove that a and b are relatively prime if and only if there exist integers x, y for which ax + by = 1.
4. Euclid’s lemma: Prove that if c divides ab and c is prime then c divides a or c divides b.

Is this statement still true if one removes the hypothesis that c is prime?

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

1. State Fermat’s theorem.
2. Using Fermat’s theorem show that 17 is a divisor of 11104 + 1.
3. State the Fundamental Theorem of Arithmetic.
4. Given non-zero integer a, prove that gcd(a, a+1) = 1



[Course Home Page](http://www.math.luc.edu/~ajs/courses/201fall2015/index.pdf) [Department Home Page](http://www.math.luc.edu/) [Loyola Home Page](http://www.luc.edu/)