Homework Assignment 6

Due on Monday, October 30, 2017.

Problem 1: Elliptic curve parameters

Consider the elliptic curve with parameters a, b, and p defined by

$$y^2 \equiv x^3 + ax + b \pmod{p},$$

For each parameter triple (a, b, p), say whether or not the resulting elliptic curve satisfies the definition for an elliptic curve modulo a prime given on slide 10 of lecture 13, and explain your answers.

	a	b	p
i.	1	0	3
ii.	3	-2	7
iii.	0	0	13
iv.	0	3	15
v.	0	3	17

Problem 2: Elliptic curve group

List all points in the elliptic curve group defined by

$$y^2 \equiv x^3 + 1 \pmod{5}.$$

Problem 3: Elliptic curve addition

The points $P = (0, 3)$ and $Q = (4, 2)$ are in the elliptic curve group defined by

$$y^2 \equiv x^3 + 4x + 4 \pmod{5}.$$

(See slide 14 of lecture 13.) What is $P + Q$? Show your work.

Problem 4: Zero divisors

An element $a \in \mathbf{Z}_n - \{0\}$ is said to be a *zero divisor* modulo n if $ab \equiv 0 \pmod{n}$ for some $b \in \mathbf{Z}_n - \{0\}$.

(a) Explain why there are no zero divisors in $\mathbf{Z}_p$ when p is prime.

(b) Find a zero divisor in $\mathbf{Z}_{21}$.

(c) What is the value of the first element to repeat in the sequence

$$(3^1 \bmod 21), (3^2 \bmod 21), (3^3 \bmod 21), (3^4 \bmod 21), \ldots?$$

In all cases, justify your answers.

Problem 5: Greatest common divisor

The definition of *greatest common divisor* can be extended naturally to a sequence of numbers $(a_1, a_2, \ldots, a_k)$, not all of which are zero; namely, it is the largest integer $d \geq 1$ such that $d \mid a_j$ for all $j = 1, 2, \ldots, k$. Describe an efficient algorithm for computing $\gcd(a_1, \ldots, a_k)$, and explain why it computes the correct answer.

Problem 6: Euler's totient function

Compute $\phi(3500)$. Show your work.

Problem 7: Euler theorem

Compute $3^{907211} \bmod 3500$.

Problem 8: Extended Euclidean algorithm

Use the extended Euclidean algorithm to solve the Diaphantine equation $599x - 711y = 1$. Show the resulting table of triples as in slide 15 of lecture 14 notes.

[Note: You *may* write a program to produce the table if you wish, but these numbers are small enough to make it quite feasible to carry out the computation by hand or with the aid of a pocket calculator.]