WORKSHEET #13 – MATH 5405
SPRING 2016

Let's start with some short answer questions.

(1) If P, Q are distinct points on an elliptic curve E and $7P + Q = 8Q$, what is the order of $P - Q$.

(2) How would Caesar encrypt the word CAT?

(3) If you receive a message encrypted with the Vigenére cipher, describe with a diagram how you would determined the key length.

(4) How many elements does the finite field $\mathbb{Z}/7\mathbb{Z}[x]/x^3 + 2$ have?

(5) Give an example of a number n so that $(\mathbb{Z}/n\mathbb{Z})^\times$ (the group of units modulo n) does not have a primitive root.

(6) What is the order of x in the group $\big((\mathbb{Z}/2[x])/x^3+x+1\big)^\times$? Is it a primitive root/generator?

(7) Is the polynomial $x^3 + x + 1 \in \mathbb{Z}/5[x]$ irreducible?

(8) If you are using the quadratic sieve to factor an integer $n = pq$, and you discover that $x^2 \equiv_n 81$, for some x a little bigger than $\sqrt{n}$, how would you factor n?

More short answer questions

(10) Suppose we are using the $p+1$ method to try to factor an integer $n = pq$. We pick our integer $z = 1 + i$ and we define $z_1 = z$. How do we define z_i and how do we compare it to n to factor n?

(11) Suppose that Alice and Bob are trying to find a shared key using a Diffie-Hellman key exchange. Alice picks a prime p and finds a primitive root x mod p. If Bob wants to after Bob chooses his private key b, what number should Bob share with Alice?

(12) In the AES cryptosystem, list the operations that make up a round.

(13) Consider the point $P = (1, 1)$ on the elliptic curve defined by $y^2 = x^3 - x + 1$ over the rational numbers. What is the x coordinate of $2P$?

(14) Fill in the blanks in the Miller-Rabin theorem. **Theorem** *Let n be an odd integer. Write $n - 1 = 2^k \cdot q$ where q is odd. If there exists an integer $a < n$ such that*
(1) $a^q \not\equiv_n$ [BLANK1]
(2) $a^{[\text{BLANK2}]} \not\equiv_n -1$ *for all* $i = 0, 1, \ldots, k-1$
then n is composite.

(15) If an error correcting code C has Hamming distance $d(C) = 7$, what is the most number of errors that C can reliably correct?

(16) Give an example of a code that can detect a single error.

(17) In a linear code C which is generated by the rows of $[I_k|P]$, how do we make the parity check matrix H so that $\mathbf{v}H^T = 0$ if and only if $\mathbf{v} \in C$.

Let's explore some ciphers. We start with the theory behind RSA.

(17) Suppose $n = pq$ is the product of two primes. If Alice publishes n and a public key e (an exponent). Bob encrypts a message m by computing $c = m^e \bmod n$. How does Alice decrypt c? Give a short proof that the procedure really does recover m (for $m < \min(p, q)$).

(18) The following ciphertext was created using a columnar transposition with the keyword `MEOW`. What was the original message?

`HTHTEKTATAMCEIECBHCNHAAU.`

(19) I applied a Vigenére cipher to `THECATCAMEBACK` and obtained `UHPNBTNLNEMLDK`. What was the keyword?

Modular arithmetic / elliptic curves.

(20) Find all the points on elliptic curve E defined by $y^2 = x^3 + 3x$ over $\mathbb{Z}/5$.

(21) Consider the points $P = (1, 2)$ and $Q = (0, 0)$ on the elliptic curve E from the previous problem. Compute $2P + Q$.

(22) Compute the inverse of the polynomial $1 + x$ in the field $(\mathbb{Z}/5[x])/(x^2 + 2)$.

Finally, we explore coding theory.

(23) Write down a parity check matrix H for a Hamming [7,4] code.

(24) If you receive a message $m = (1, 0, 0, 0, 1, 1, 0)$ what was the intended message, or can you tell?

(25) If C is the cyclic binary code of length 6 with generating polynomial $g(x) = x^2 + x + 1$. Find two elements in C and find two elements not in C.