EECS 70 Discrete Mathematics and Probability Theory
Spring 2013 Anant Sahai

HW 5

Due Feb 25

1. Polynomials and modular arithmetic

Which of the following statements is true? In each case, if the statement is true give a brief explanation; if it is false, give a simple counterexample.

1. For all $a, b \in \mathbf{Z}$, $(a+b)^3 = a^3 + b^3 \mod 3$.
2. For all $a, b \in \mathbf{Z}$, $(a+b)^4 = a^4 + b^4 \mod 4$.
3. For all $a, b \in \mathbf{Z}$, $(a+b)^5 = a^5 + b^5 \mod 5$.

2. More polynomials!

Define the sequence of polynomials by $P_0(x) = x + 12$, $P_1(x) = x^2 - 5x + 5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$. (For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.)

1. Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in \mathbb{N}$.
2. Show that, for every prime q, if $P_{2013}(x) \not\equiv 0 \pmod{q}$, then $P_{2013}(x)$ has at most 2013 roots modulo q.

3. Solving systems of equations

Consider the following system of equations $\mod 15$:

$$\begin{aligned} 13x + 7y &= 2 \\ 3x + 4y &= 8 \end{aligned}$$

1. Decompose this into two systems of equations, one $\mod 3$ and one $\mod 5$.
2. Solve for x and y in both systems.
3. Combine these solutions to get a solution to the original problem (hint: look at discussion 3, problem 5a)

4. You be the grader

Would you give this proof an A or an F?

Claim: Let m be any natural number with $m > 1$ and x, y be integers. If $x^4 + y^4 \equiv 2x^2y^2 \pmod{m}$, then either $x \equiv y \pmod{m}$ or $x \equiv -y \pmod{m}$.

Proof: Suppose x, y form an integer solution to the equation, so we are given

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

Subtracting $2x^2y^2$ from both sides, we find that

$$x^4 - 2x^2y^2 + y^4 \equiv 0 \pmod{m}.$$

We can factor the left-hand side, to get

$$(x^2 - y^2)^2 \equiv 0 \pmod{m}.$$

Taking the square root of both sides, we see that

$$x^2 - y^2 \equiv 0 \pmod{m},$$

or in other words,

$$x^2 \equiv y^2 \pmod{m}.$$

Taking the square root of both sides again, we find that either $x \equiv y \pmod{m}$ or $x \equiv -y \pmod{m}$ (we have to include both possibilities, because the square root on each side could be either positive or negative). This proves the claim.

5. Wait... We don't need to play at the same time?

In the two player game of "Rock, Paper, Scissors", each player chooses one of these three symbols and both reveal their choice simultaneously. If the symbols are the same, the game is a tie; otherwise rock beats scissors, scissors beats paper, or paper beats rock.

1. Suppose Alice and Bob want to play Rock, Paper, Scissors over instant messenger. What problems might they run into?
2. Using public key cryptography, can you devise a system whereby Alice and Bob can play the game over an asynchronous channel, with no third party to mediate? Analyse the security of your system.

   (Hint: consider a system where player Alice chooses a symbol and sends message (1) to Bob containing proof of that choice (but without immediately saying what the choice was, since that would ruin the game). Bob then chooses a symbol and sends message (2) back to Alice, who works out who won and sends message (3) to Bob, either accepting defeat or using (1) to prove that Alice won this round.)

6. Do question 1 on the midterm.

7. Do question 2 on the midterm.

⋮

5+n. Do question n (the last question) on the midterm.