EECS 70 Discrete Mathematics and Probability Theory
Spring 2014 Anant Sahai Discussion 6B

1. What's your number? (...Oh, what's the point?!)

Your GSI has (let us imagine) chosen to distribute a secret number s among 10 students, with s being one of the eleven values from 0 through 10. The way your GSI distributed this secret is by choosing a polynomial $P(x)$ of degree ≤ 2 such that $P(0) \equiv s \pmod{11}$. They then told their favorite student the value of $P(1)$ modulo 11, their second favorite student the value of $P(2)$ modulo 11, and so on, up through $P(10)$.

1. Suppose you were told that $P(6) \equiv 7 \pmod{11}$ and your neighbor was told that $P(7) \equiv 5 \pmod{11}$. What can the two of you determine about s from this information?
2. You and your neighbor begin speculating about what the eighth-favorite student heard from the GSI. What can the two of you determine about the value of P(8)?
3. Suppose that the eighth-favorite student, hearing your whispers, comes along and tells you outright that $P(8) \equiv 4 \pmod{11}$. What can the three of you determine about s now?
4. Were a wave of amnesia to suddenly hit parts of the classroom, how many students would need to retain their memories in order to be able to re-determine the values each student received from the GSI?

2. Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination s. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

1. Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.
2. The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country. (Hint: use $n+1$ polynomials.)

3. E_ror Cor_ecti_n

Consider the alphabet $A = 0$, $B = 1$, $C = 2$, $D = 3$, $E = 4$. Suppose a message of length 3 is sent using the error correction scheme discussed in class over $GF(5)$, with no more than one erasure. If you receive the following packets, what was the original message?

1. C _ A A
2. _ A C C
3. C E _ C