CS 70 Challenge Problems: Modular Arithmetic and Polynomials

Solutions at https://alextseng.net/teaching/cs70/

Alex Tseng

---

1 Modular Arithmetic

(a) Let p be a prime number ($p > 2$). Recall that a perfect square y is such that there exists an integer x where $x^2 = y$. With a modulus, a perfect square y is such that there exists an integer x where $x^2 \equiv y \pmod{p}$. Then that makes x the square root of y. Prove that for any $a \in \{1, 2, ..., p-1\}$, a has either 0 or 2 distinct square roots (mod p).

(b) Prove that there are exactly $\frac{p+1}{2}$ perfect squares (mod p).

(c) *Challenge* Prove that there are *at least* $\frac{p}{3}$ perfect *cubes* (mod p).

(d) *Challenge* Digit the cybird has sent a coded message with Motherboard access codes using RSA to Inez, Jackie, and Matt. He sends them each a copy of the same message. Inez, Jackie, and Matt each have their own set of public keys: $(N_I, e_I), (N_J, e_J), (N_M, e_M)$. It turns out that all three of them have selected the same encryption exponent $e_I = e_J = e_M = 3$. Additionally, Digit is quite terse in his message m, so that it is smaller than each of the public key moduli: $m < N_I, N_J, N_M$. Hacker has intercepted all three encrypted messages E_I, E_J, E_M, and wishes to decipher the access codes. Show how he can do this efficiently (without factoring the public keys).

2 Polynomials

(a) Find a polynomial *of lowest degree* that satisfies the following congruences:
$P(0) \equiv 4 \pmod 7$
$P(2) \equiv 5 \pmod 7$
$P(4) \equiv 0 \pmod 7$

(b) Consider a function $d(n)$, which takes in a natural number n (in base 10), cubes all of the digits, and adds them up. For example, $d(24) = 2^3 + 4^3 = 8 + 64 = 72$. Prove that $d(n) = n \pmod 3$ for all $n \in \mathbb{N}$.

(c) The engineering team of m people at Quince is about to release their newest model of qPhones. In order to guard against any overly-excited engineers from prematurely releasing the qPhone before the agreed-upon release date, the team decides lock up all of the qPhones in a safe with a secret code. Only the entire engineering team together should be able to open the safe. However, it has been suspected that one of the engineers is really a corporate spy, whose mission is to delay—or even cancel—the release of the qPhone. Devise a mechanism so that the engineering team can protect against premature-releases, while still being able to open the safe on time, even in the presence of a spy.