Mathematics 342, Term 2, 2018. Instructor: Reichstein.

Problem set 2. Due Thursday, February 1

(1) Show that if there exists a q-ary (n, M, d)-code for some $2 \leq d \leq n$, then there exist a q-ary $(n, M, d-1)$-code.

(2) What is $A_2(n+1, n)$? Consider every integer $n \geq 1$.

(3) In each case construct, if possible, a binary (n, M, d)-code. If no such code exists, explain why. You can use any of the coding bounds we have covered in class.

(a) $(n, M, d) = (7, 2, 7)$,

(b) $(n, M, d) = (5, 3, 4)$,

(c) $(n, M, d) = (6, 4, 4)$,

(d) $(n, M, d) = (4, 8, 2)$,

(e) $(n, M, d) = (8, 29, 3)$.

(4) Without using a computer, a calculator, or Fermat's theorem, find the following principal remainders.

(a) $513418^{100000} \pmod{17}$,

(b) $99^{101} \pmod{31}$,

(c) $263912^{20111} \pmod{13}$.

(5) Use the Euclidean algorithm to find $15^{-1} \pmod{37}$.

(6) Let $\gcd(a, b, c)$ denotes the the greatest common divisor of three integers a, b, c. Let us assume that $a > 0$.

(a) Show that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

(b) Explain why there exist integers x, y, z such that $ax+by+cz = \gcd(a, b, c)$ and how to find them using the Euclidean algorithm.

(c) Use your method to find integers x, y, z such that $15x + 10y + 6z = 1$.

(7) Show that the congruence $x^2 \equiv 1 \pmod{n}$ has exactly two solutions, $x \equiv -1$, and $x \equiv 1 \pmod{n}$, assuming that $n = p$ is an odd prime number. (Here we do not distinguish between solutions that are congruent modulo n. For example, if $n = 3$ then $x = 1$ and $x = 4$ are considered the same.)

(8) (a) Use Problem 7 to show that $(p-1)! \equiv -1 \pmod{p}$ for every prime number p. (This congruence is called Wilson's theorem.)

Hint: In the product $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ to pair up each element x with its multiplicative inverse x^{-1} in $\mathbb{Z}_p$.

(b) Show by example that Wilson't theorem may fail if n is not a prime.