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

Solutions to Problem Set 2.

(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.

Solution: We will start with a q-ary (n, M, d)-code C and construct a q-ary $(n, M, d-1)$-code C'.

Choose $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$ in C such that $d(\mathbf{a}, \mathbf{b}) = d$ is the smallest possible. That is, $\mathbf{a}$ and $\mathbf{b}$ differ in exactly d positions. Suppose one of these d positions is position i, i.e., $a_i \neq b_i$. Modify $\mathbf{a}$ by replacing a_i by b_i. Denote the resulting word by $\mathbf{a}'$. Clearly

$$(*) \qquad d(\mathbf{a}', \mathbf{b}) = d - 1\,.$$

Let C' be the code obtained by changing $\mathbf{a}$ to $\mathbf{a}'$ and leaving the remaining words in C unchanged. Then C' has the same number of words as C. It remains to show that $d(C') = d - 1$.

First note that $d(C') \leq d - 1$ by $(*)$; this was, in fact, the entire point of replacing $\mathbf{a}$ by $\mathbf{a}'$. Thus we only need to show that

$$d(C') \geq d - 1,$$

i.e., $d(\mathbf{x}, \mathbf{y}) \geq d - 1$ for any distinct words $\mathbf{x}$ and $\mathbf{y}$ in C'. Indeed, if neither of these words is $\mathbf{a}'$, then both $\mathbf{x}$ and $\mathbf{y}$ are words in C. Thus

$$d(\mathbf{x}, \mathbf{y}) \geq d(C) = d > d - 1,$$

as desired. On the other hand, if one of these words in $\mathbf{a}'$, say, $\mathbf{x} = \mathbf{a}'$, then by the triangle inequality,

$$d \leq d(\mathbf{a}, \mathbf{y}) = d(\mathbf{a}, \mathbf{a}') + d(\mathbf{a}', \mathbf{y}) = 1 + d(\mathbf{x}, \mathbf{y}).$$

Subtracting 1 from both sides, we obtain

$$d - 1 \leq d(\mathbf{x}, \mathbf{y}).$$

This shows that $d(C') = d - 1$.

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

Solution: We have shown in class that $A_2(n+1, 1) = 2^{n+1}$ and $A_2(n+1, 2) = 2^n$. This takes care of $n = 1$ and $n = 2$:

$$A_2(2, 1) = A_2(3, 2) = 2^2 = 4.$$

From now on, assume $n \geq 3$. I claim that in this case $A_2(n+1, n) = 2$. Clearly $A_2(n+1, n) \geq 2$, since the 2-word code $\{(0, \dots, 0, 0), (1, \dots, 1, 0)\}$ of length $n+1$ has minimal distance n. It thus remains to prove that a code C of length $n+1$ and minimal distance $\geq n$ cannot have more than two words. After replacing C by an equivalent code, we may assume that C contains $\mathbf{0} = (0, \dots, 0)$. Any other word $\mathbf{x}$ in C will have weight (i.e., distance from $\mathbf{0}$) $\geq n$. Equivalently, $d(\mathbf{x}, \mathbf{1}) \leq 1$,

where $\mathbf{1}$ is the all-one word $(1, 1, \ldots, 1)$. If C has two non-zero words, say $\mathbf{x}$ and $\mathbf{y}$, then by the triangle inequality

$$d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{1}) + d(\mathbf{1}, \mathbf{y}) \leq 1 + 1 = 2 \leq n\,,$$

a contradiction. (Recall that we are assuming that $n \geq 3$.) This shows that C cannot have more than two words.

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

Solution: (a) The repetition code $\{(0000000), (1111111)\}$ is a binary $(7, 2, 7)$-code.

(b) By Problem 2, $A_2(5, 4) = 2$. This means that a binary code of length 5 and minimal distance 4 has at most 2 words. Thus a binary $(5, 3, 4)$-code cannot exist.

(c) Add a parity check digit to the binary $(5, 4, 3)$-code C_3 in Example 1.5 in the book to obtain the binary $(6, 4, 4)$-code

$$\{(000000), (011011), (101101), (110110)\}.$$

(d) The binary code consisting of all words of length 4 of even weight,

$$\{(0000), (0011), (0101), (0110), (1001), (1010), (1100), (1111)\},$$

is a $(4, 8, 2)$-code.

(e) Impossible by the Hamming bound, since $\dfrac{2^8}{1+8} = 28.444\ldots < 29$.

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

Solution: (a) $513418 \equiv 51 \cdot 10^4 + 34 \cdot 10^2 + 18 \equiv 1 \pmod{17}$. Thus

$$513418^{100000} \equiv 1^{100000} \equiv 1 \pmod{17}.$$

(b) $99 \equiv 6 \pmod{31}$. On the other hand, $6^2 \equiv 36 \equiv 5 \pmod{31}$ and thus $6^3 \equiv 5 \cdot 6 \equiv -1 \pmod{31}$. We conclude that

$$99^{101} \equiv 6^{101} \equiv (6^3)^{33} \cdot 6^2 \equiv (-1)^{33} \cdot 36 \equiv -5 \equiv 26 \pmod{31}.$$

(c) Since $263912 \equiv 26 \cdot 10^4 + 39 \cdot 10^2 + 12 \equiv -1 \pmod{13}$, we have

$$263912^{20111} \equiv (-1)^{20111} \equiv -1 \equiv 12 \pmod{13}\,.$$

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

Solution:
We perform the Euclidean algorithm on the pair $(15, 7)$:

$37 = 15 \cdot 2 + 7,$

$15 = 7 \cdot 2 + 1.$

Back substitution:

$$1 = 15 - (37 - 15 \cdot 2) \cdot 2 = 15 \cdot 5 - 37 \cdot 3\,.$$

Reducing both sides modulo 37, we see that $1 \equiv 15 \cdot 5 \pmod{37}$. Thus $15^{-1} \equiv 5 \pmod{37}$.

(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 $15x + 10y + 6z = 1$.

Solution: (a) It is enough to show that (a, b, c) have the same common divisors as $(\gcd(a, b), c)$.

Suppose d divides both $\gcd(a, b)$ and c. Then clearly d divides a, b and c.

Conversely, suppose e divides a, b, and c. Then since $\gcd(a, b)$ can be written as $sa + tb$, for some integers s and t, e also divides $\gcd(a, b)$. Thus e divides both $\gcd(a, b)$ and c.

We have thus shown that that (a, b, c) and $(\gcd(a, b), c)$ have the same common divisors. Hence, they also have the same greatest common divisor.

(b) First we find integers s and t so that $as + bt = \gcd(a, b)$. This can be done using the Euclidean algorithm and back substitution, as in Problem 5 above. Then, in a similar manner, we find integers v and z so that $\gcd(a, b)v + cz = \gcd(\gcd(a, b), c)$. Now $\gcd(a, b, c) =$

$$\gcd(\gcd(a, b), c) = \gcd(a, b)v + cw = (as + bt)v + cz = a(sv) + b(tv) + cz\,.$$

(c) Here $\gcd(15, 10) = 5$ and $\gcd(5, 6) = 1$. We write $5 = 15 - 10$ and $1 = 6 - 5$. Now

$1 = 6 - 5 = 6 - (15 - 10) = 15 \cdot (-1) + 10 \cdot (1) + 6 \cdot (1).$ □

(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.)

Solution: Rewrite $x^2 \equiv 1 \pmod{n}$ as $x^2 - 1 \equiv (x - 1)(x + 1) \equiv 0 \pmod{n}$. Since $\mathbb{Z}_n$ is a field if n is prime we have $ab = 0$ implies $a = 0$ or $b = 0$. Thus in our case $(x - 1) \equiv 0 \pmod{n}$ or $(x - 1) \equiv 0 \pmod{n}$; in other words $x \equiv 1$ or $x \equiv -1$. Note that these two solutions are distinct if $n > 2$ (i.e there's only one solution for n the even prime 2).

(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.

Solution: (a) For $p = 2$ the identity is clear $1! = 1 \equiv -1 \pmod{2}$. Now suppose $p \geq 3$. Since we are working over a field, each element has a unique inverse. By (a) the only elements that are their own inverses are $x \equiv 1$ or $x \equiv -1$. Changing the order of the factors and grouping pairs of inverses gives us $(p-1)! \equiv (x \cdot x^{-1})(y \cdot y^{-1}) \cdots (z \cdot z^{-1}) \cdot (1)(-1) \equiv -1 \pmod{n}$.

(b) Suppose $n = ab$ for some integers $2 \leq a, b \leq n-1$. Then $(n-1)!$ is divisible by a; hence, can never be $-1 \pmod{n}$. For example, for $n = 4$, $(n-1)! = 3! = 1 \cdot 2 \cdot 3 \equiv 2 \pmod{4}$.