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

\[
(d(a', b)) = d - 1.
\]

Let \( C' \) be the code obtained by changing \( a \) to \( a' \) 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 \( a \) by \( a' \). Thus we only need to show that

\[
d(C') \geq d - 1,
\]

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

\[
d(x, y) \geq d(C) = d > d - 1,
\]

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

\[
d \leq d(a, y) = d(a, a') + d(a', y) = 1 + d(x, y).
\]

Subtracting 1 from both sides, we obtain

\[
d - 1 \leq d(x, y).
\]

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 \( \{(0, \ldots, 0, 0), (1, \ldots, 1, 0)\} \) of length \( n+1 \) has minimal distance \( n \). It thus remains to prove that \( A_2(n+1, n) \geq 2 \), i.e., a code \( C \) of length \( n+1 \) and minimal distance \( \geq n \) cannot have more than two words. We will prove this in two ways.
1. Apply the Plotkin bound:

\[ A_2(n + 1, n) \leq 2 \cdot \left\lfloor \frac{n}{2n - (n + 1)} \right\rfloor = 2 \cdot \left\lfloor \frac{n}{n - 1} \right\rfloor = 2 \cdot \left\lfloor 1 + \frac{1}{n - 1} \right\rfloor = 2. \]

Note that \( \frac{1}{n - 1} < 1 \) for any \( n \geq 3 \).

2. Use a direct argument. After replacing \( C \) by an equivalent code, we may assume that \( C \) contains \( \textbf{0} = (0, \ldots, 0) \). Any other word \( \textbf{x} \) in \( C \) will have weight (i.e., distance from \( \textbf{0} \)) \( \geq n \). Equivalently, \( d(\textbf{x}, \textbf{1}) \leq 1 \), where \( \textbf{1} \) is the all-one word \( (1, 1, \ldots, 1) \). If \( C \) has two non-zero words, say \( \textbf{x} \) and \( \textbf{y} \), then by the triangle inequality

\[ d(\textbf{x}, \textbf{y}) \leq d(\textbf{x}, \textbf{1}) + d(\textbf{1}, \textbf{y}) \leq 1 + 1 = 2 \leq n, \]

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) \(\{(00000), (11100), (00111), (11011)\}\) is a binary \((5, 3, 4)\)-code.

(c) Add a parity check digit to the code in part (c):

\[\{(0000000), (1111000), (0011111), (1100111)\}\]

is a binary \((6, 4, 4)\)-code.

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

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

is a binary \((4, 8, 2)\)-code.

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

(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 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 $a, b, c$. 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

$$1 = 6 - 5 = 6 - (15 - 10) = 15 \cdot (-1) + 10 \cdot 1 + 6 \cdot 1.$$ \[\square\]
(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 $b = 0$. In our case this means that $x - 1 \equiv 0 \pmod{n}$ 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 $n > 2$. There’s only one, $x = 1$ for $n = 2$.

(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.)

**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 $(p - 1)! \equiv (1)(1)(1)(1) \cdots (1)(-1) \equiv -1 \pmod{n}$.

(b) Show by example that Wilson’s theorem may fail if $n$ is not a prime.

**Solution:** (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 $n = 4$, $(n - 1)! = 3! = 1 \cdot 2 \cdot 3 \equiv 2 \pmod{4}$.