

10. MATH 30A, HOMEWORK 10 REVISED

Now due: Monday, Nov 30. This is the last homework.

The problems are the same, the hints are different.

- (1) (#28 on page 190) Show that $(p-1)!$ is congruent to -1 modulo p for any prime p . [Use the previous problem #27 which says that the only elements of \mathbb{Z}_p^\times which are their own inverses are 1 and $p-1$.]
- (2) Find all the units in the ring \mathbb{Z}_{35} which are equal to their own inverses. [Hint: Use the formula $\mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_7$, look at #27 on page 190. The case $(4, 1)$ is done on the next page.]
- (3) Imitating the construction of $GF(16)$, list the 4 elements of $GF(4)$, giving them appropriate names or notation, describe the addition and multiplication rules and then fill in the complete 4×4 multiplication table.
- (4) For any field F of characteristic 2, show that the function

$$\Phi(x) = x^2$$

is an automorphism $\Phi : F \rightarrow F$. (*Automorphism* means isomorphism from a group or ring to itself.) The automorphism Φ is called the *Frobenius*.

- (5) Find the elements of $GF(16)$ which make up the unique subfield with 4 elements. [These 4 elements are the solutions of the equation $X^4 = X$. It is helpful to look on the bottom of page 16 where I explained that $x = 1010$ generates $GL(16)^\times$.]
- (6) Take the polynomial $f(x) = x^4 + 3x^3 + 2x^2$ considered as a polynomial with coefficients in $GF(5) = \mathbb{Z}_5$. Divide by $g(x) = x^2 + 1$. What is the quotient and remainder? Make sure all coefficients are in the set $\{0, 1, 2, 3, 4\}$ (no negative number and no numbers bigger than 4). Show that the remainder divides $g(x)$. Conclude that the remainder (divided by the leading coefficient) is the greatest common divisor of $f(x)$ and $g(x)$.
- (7) Take the additive group $G = \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7$. Suppose that $a, b \in G$ are fixed elements having the property that a is not a multiple of b and b is not a multiple of a . Then show that there are exactly 49 elements of G which are integer linear combinations of a and b . In other words, show that the set

$$\{na + mb \mid n, m \in \mathbb{Z}\}$$

has cardinality 49. Hints: this set is a subgroup of G with at most 49 elements. The reason is that $7a = 7b = 0$ and therefore

$$\{na + mb \mid n, m \in \mathbb{Z}\} = \{na + mb \mid n, m \in \mathbb{Z}_7\}$$

For problem #2, we have the isomorphism

$$\phi : \mathbb{Z}_{35} \rightarrow \mathbb{Z}_5 \times \mathbb{Z}_7$$

given by

$$\phi(x) = (x \bmod 5, x \bmod 7)$$

One of the solutions of this problem is the element $(4, 1) \in \mathbb{Z}_5 \times \mathbb{Z}_7$. To find the element of \mathbb{Z}_{35} which corresponds to this we need to know that:

$$\boxed{5(3) + 7(-2) = 1}$$

Why does this help? We are looking for the number $x \in \mathbb{Z}_{35}$ so that

$$x \equiv 4 \pmod{5}$$

$$x \equiv 1 \pmod{7}$$

In other words,

$$x = 4 + 5a$$

$$x = 1 + 7b$$

But then

$$4 + 5a = 1 + 7b$$

$$3 = 5(-a) + 7(b)$$

Can we find a, b ? Yes, we just multiply the boxed equation by 3 to get:

$$3 = 5(9) + 7(-6)$$

So, $a = -9$ and $b = -6$. This makes

$$x = 4 + 5a = 4 - 45 = -41 = 29 \in \mathbb{Z}_{35}$$

Let's check this:

$$29^2 = 35(24) + 1 = 1 \in \mathbb{Z}_{35}$$