Math 117 **S04 SOLNS4.**

Solutions to Assignment #4

p. 84, E1: In $\mathbb{Z}/14\mathbb{Z}$, omitting brackets we get 12 + 8 = 6, 6 + 5= 11, 10 + 5 = 1, $12 \cdot 8 = (-2) \cdot (-6) = 12$, $6 \cdot 5 = 2$, $10 \cdot 5 = 8$.

p. 84, E3:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

p. 86, E3: In $\mathbb{Z}/13\mathbb{Z}$, $\{0, 1, 2, 2^2, \ldots, 2^{12}\} = \{0, 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$, which is a complete set of representatives. Notice that after you hit $12 = -1$ in the middle, the last half will be the negatives of the first half.

(In such problems, the text lists the primitive element and then its powers, ending with 1. I think it's more meaningful to list the 0-th power first, so $1, 2, 4, \ldots$.)

p. 86, E4: We usually try 2 first ; if that doesn't work, then 3; if that doesn't work then 5 (skipping 4 since it has been seen as a power of 2), etc.

(i) For $m = 5$, 2 is primitive since its powers are $1, 2, 4, 3$.

(ii) For $m = 7$, 2 is not primitive since $2^3 = 1$, but 3 is primitive since its powers are $1, 3, 2, 6, 4, 5$.

(iii) For $m = 11$, 2 is primitive since its powers are $1, 2, 4, 8, 5, 10, 9, 7, 3, 6$.

p. 89, E4: In $\mathbb{Z}/14\mathbb{Z}$ we have units $1, 3, 5, 9, 11, 13$, related by $1 \cdot 1 = 1$, $3 \cdot 5 = 1$, $9 \cdot 11 = 1$, $13 \cdot 13 = 1$.

p. 90, E8: I think it's best to do these problems by replacing any integers by easier residues, converting to an equation, dividing by the gcd of all integers in sight, and going from there.

Remember, these are all in $\mathbb{Z}/12\mathbb{Z}$, so $[a] = [4]$ when $4 - a$ is a multiple of 12, i.e., $4 - a = 12y$ for some y, which is the same as $a + 12y = 4$ for some y.

Also, remember that for an equation $ar + bs = c$, any particular solution r, s gives more solutions by replacing r by $r + kb$ and s by $s - ka$, for each k. If a and b are coprime then this gives all solutions.

(i) Solving $[4]x = [18] = [6]$ is equivalent to solving $4x+12y = 6$ or $2x+6y = 3$, which is impossible, so there are no solutions.

(ii) Solving $[9]x = [48] = [0]$ is equivalent to solving $9x+12y = 0$ or $3x+4y = 0$. One solution is $x = 0, y = 0$; all solutions are $x = 0 + 4k, y = 0 + -3k$ for each k. So in the original problem, $x = [4k]$ for each k. This expression takes on only three different values: $x = [0], [4], [8]$.

(iii) Solving $[10]x = [100]$ is the same as $[-2]x = [4]$, which is equivalent to solving $-2x + 12y = 4$ or $x - 6y = -2$. One solution is $x = -2, y = 0$. All solutions are $x = -2 + 6k, y = -k$ for each k. So solutions to the original problem are $x = -2 + 6k$ as k varies. There are only two distinct values, $x = [4], [10]$ (where $[10] = [-2]$).

p. 90, E9: Following the same ideas as in the preceding solution, but for $\mathbb{Z}/30\mathbb{Z}$:

(i) $[4]x = [18]$ is the same as $4x + 30y = 18$ or $2x + 15y = 9$. Instead of using the Euclidean algorithm, notice that $2\cdot 8+15\cdot(-1) = 1$ so $2\cdot 72+15\cdot(-9) = 9$ and the general solution is $x = 72 + 15k, y = -9 - 2k$. The least positive residues for x occur when $k = -3, -4$ and we get $x = [12], [27]$.

(ii) $[9]x = [48] = [18]$ is the same as $9x + 30y = 18$ or $3x + 10y = 6$. One solution is $x = 2, y = 0$, the general solution is $x = 2 + 10k, y = 0 - 3k$, and the least-residue solutions to the original problem are $x = [2], [12], [22]$.

(iii) $[10]x = [100] = [10]$ is the same as $10x+30y = 10$ or $x+3y = 1$. One solution is $x = 1, y = 0$, the general solution is $x = 1+3k, y = -k$, and the least positive residues for x are $x = [1], [4], [7], [10], [13], [16], [19], [22], [25], [28]$.

(iv) $[12]x = 8$ is the same as $12x + 30y = 8$ or $6x + 15y = 4$, which has no solution since the l.h.s. is divisible by 3 and the r.h.s. is not.

(v) $[6]x = 2$ is the same as $6x + 30y = 2$ or $3x + 15y = 1$, which has no solution since the l.h.s. is divisible by 3 and the r.h.s. is not.

E-1: The exponent is written in binary as a reminder that one good method is repeated squaring following by putting together the pieces of the exponent: The exponent is $16 + 4 + 2$.

(a) $3^2 = 9, 3^4 \equiv 9^2 \equiv 1 \pmod{16}$, so $3^8 \equiv 1 \pmod{16}$ and $3^{16} \equiv 1 \pmod{16}$; we get $3^{16+4+2} \equiv 1 \cdot 1 \cdot 9 = 9 \pmod{16}$.

(b) $3^2 = 9$, $3^4 \equiv 9^2 \equiv -4 \pmod{17}$, $3^8 \equiv (-4)^2 \equiv -1 \pmod{17}$, $3^{16} \equiv (-1)^2 = 1 \pmod{17}$, so $3^{16+4+2} \equiv 1 \cdot (-4) \cdot 9 = -36 \equiv -2 \equiv 15 \pmod{17}$. (As a shortcut, notice that 3^{16} has to be $\equiv 1 \pmod{17}$ by Little Fermat.)

E-2: First, notice that every odd integer is of the form $4n+1$ or $4n-1$, so is $\equiv 1 \pmod 4$ or $\equiv -1 \pmod 4$.

(a) How about a sum of two squares, a^2+b^2? Modulo 4, the only squares are 0 and 1, so a^2+b^2 must be $\equiv$ to one of 0, 1, or $1+1=2 \pmod 4$, never 3 $(\equiv -1)$. For $p = a^2+b^2$, either p is even, so $p = 2 = 1^2+1^2$, or else p is odd, so is $\equiv 1 \pmod 4$, i.e., $p = 4n+1$ for some n.

(b) $29 = 2^2+5^2$; $61 = 5^2+6^2$; $97 = 4^2+9^2$.

E-3: (a) Because $\sqrt{2}$ is a root of x^2-2 and is not an integer. In general, $\sqrt{n}$ is a root of x^2-n and so is either an integer or irrational.

Note: How to justify that $\sqrt{2}$ is not an integer? Either point out that $\sqrt{1}=1$ and $\sqrt{4}=2$ and so $\sqrt{2}$ is between 1 and 2, or mention that 2 is prime while a perfect square would have a prime factorization in which each prime has an even exponent.

(b) As suggested: Suppose $\frac{a}{b}$ is in lowest terms (i.e., that a, b are coprime—and to allow the fraction to be negative, let's assume that $b > 0$ while a can be positive or negative) and also is a root of $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ with integer coefficients. We want to show that $b = 1$ so $\frac{a}{b}$ will be an integer. Start from the equation

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\frac{a}{b} + c_0 = 0.$$

Multiply through by b^n and solve for a^n; we get

$a^n = -c_{n-1}a^{n-1}b - \cdots - c_1ab^{n-1} - c_0b^n = -b(c_{n-1}a^{n-1} + \cdots + c_1ab^{n-2} + c_0b^{n-1})$.

Thus any prime divisor of b also divides a^n and hence a. This would contradict the fact that a and b are coprime, unless $b = 1$. Therefore $b = 1$ and so $\frac{a}{b}$ is an integer. □

The point of the theorem is that a number that is a root of a polynomial like this is never a fraction that is not an integer, e.g., $\frac{5}{8}$.

(c) We can apply the theorem by finding a polynomial of which the given number is a root. Write $r = \sqrt{\sqrt{5}+1}$ and square, getting $r^2 = \sqrt{5}+1$. Squaring again doesn't get rid of the square root on the right; instead, move the "1" to the left side and square: $r^2-1=\sqrt{5}$, $(r^2-1)^2 = 5$. Now move the 5 to the left side and simplify: $r^4-2r^2-4=0$. So r is a root of x^4-2x^2-4, which is a polynomial with integer coefficients and leading coefficient 1. The theorem says that r is either irrational or an integer. One way to see that it is not an integer is to point out that $\sqrt{\sqrt{0}+1} = 1$ and is smaller than r, while $\sqrt{\sqrt{9}+1} = 2$ and is larger than r.

E-4: (a) $b^n - 1 = (b-1)(1+b+b^2+\cdots+b^{n-1})$, so b can't be prime unless one of the factors is 1, which means either that $b = 2$ or that $1 + b + \ldots b^{n-1} = 1$, which doesn't happen for $b > 0$ and $n > 1$.

(b) If $n = rs$ with $r, s > 1$ then $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1$, which is not prime by (a) with $b = 2^r$.

(c) Experimentation gives $M_{11} = 23 \cdot 89$, which is not prime.

E-5: (a) If b is odd and $n \geq 1$ then b^n is odd and so $b^n + 1$ is even. The only even prime is 2, which happens only if $b = 1$. [The problem should have said that $b > 1$.]

(b) As suggested, for n odd we have $b^n + 1 = (b+1)(1 - b + b^2 - \cdots + b^{n-1})$. For $b, n > 1$, at least $b + 1 > 1$. We need to show that the other factor is not 1: If it were then $b^n + 1 = (b+1) \cdot 1$, i.e., $b^n = b$, so $b^{n-1} = 1$, so $b = 1$, which we're excluding. Therefore the second original factor is > 1 and $b^n + 1$ is not prime.

(c) If $n = rs$ with s odd, then $b^n + 1 = b^{rs} + 1 = (b^r)^s + 1$, which fits part (b) with b^r in place of b, so $b^n + 1$ is not prime.

Then as the problem says, n is a power of 2, so we are considering numbers of the form $b^{2^k} + 1$. The most popular value of b to use is 2, although other values will give primes some of the time also; e.g., $6^2 + 1 = 37$, which is prime.

(d) For $F_k = 2^{2^k} + 1$, we have $F_5 = 641 \cdot 6700417$.