

Assignment 3

Evan Curry Wilbur

March 16, 2023

5.01

Compute $1 + 1 + 1 + 1 + 1$ in the finite field \mathbb{F}_2 .

Solution.

$$1 + 1 + 1 + 1 + 1 = 1.$$

□

5.02

Compute

$$\underbrace{1 + 1 + 1 + \cdots + 1}_{107}$$

in the finite field \mathbb{F}_2 .

Solution.

$$\underbrace{1 + 1 + 1 + \cdots + 1}_{107} = 1.$$

□

5.03

Compute $(1 + x + x^2)^4$ as a polynomial with coefficients in \mathbb{F}_2 .

Solution.

Using the Freshman's dream theorem, we are actually allowed to distribute the exponent across the addition so

$$\begin{aligned}(1 + x + x^2)^4 &= 1^4 + x^4 + (x^2)^4 \\ &= 1 + x^2 + x^8\end{aligned}$$

□

5.04

Compute the product $(x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)$ in the collection of polynomials with coefficients in \mathbb{F}_2 .

Solution.

Worked this out on paper. Hopefully you can trust I did the algebra correctly since I'm too lazy to type up all the steps:

$$x^{12} + x^9 + x^6 + x^3 + 1$$

□

5.05

Let $g(x) = x^3 + x + 1$ be a generating polynomial for a CRC/ Compute the CRC for the byte 11100011.

Solution.

0000

□

5.08

Verify that the CRC with generating polynomial $1 + x^2 + x^3 + x^4$ fails to detect two-bit errors that are a multiple of 7 bits apart.

Solution.

content...

□

6.01

Factor the integers 1028 and 2057 into primes.

Solution.

$$1028 = 2^2 \times 257$$

$$2057 = 11^2 \times 17.$$

□

6.03

Find the reduction mod 88 of -1000.

Solution.

$$-1000 \cong 56 \pmod{88}.$$

□

6.07

Prove in general that if r is the reduction of $N \pmod m$, and if $r \neq 0$, then $m-r$ is the reduction of $-N \pmod m$.

Solution.

Let $r \cong N \pmod m$ where $0 < r < m$. So there exists a $q \in \mathbb{Z}$ such that $N = qm + r$. Then

$$\begin{aligned} N = qm + r &\Rightarrow -N = -qm - r \\ &= -qm - r + m - m \\ &= -(q+1)m + (m-r). \end{aligned}$$

Since $0 < r < m$ it follows that $0 < m-r$. Furthermore, $r > 0$ hence $m-r < m$. Therefore, $0 < m-r < m$ and so $m-r$ is the reduction of $-N$ modulo m . \square

6.22

Show that for any integer n , the integers n and $n^2 + 1$ are relatively prime.

Solution.

Let $d = \gcd(n, n^2 + 1)$. Then $d|n$ and $d|n^2 + 1$. But also, $d|n^2$ so it must be that $d|n^2 + 1 - n^2$ since it's just a linear combination of elements that are divisible by d . Thus $d|1$ so $d = 1$. \square

6.37

Find $\gcd(1112, 1544)$ and express it in the form $1112x + 1544y$ for some integers x and y by hand computation.

Solution.

$$\begin{aligned} \gcd(1112, 1544) &= 8 \\ 1112 \times 25 + 1544 \times -18 &= 8 \end{aligned}$$

\square

6.49

Compute and *reduce modulo* the indicated *modulus*: $110 \times 124 \pmod 3$ and also $12 + 1234567890 \pmod{10}$.

Solution.

$$\begin{aligned} 110 \times 124 \pmod 3 &\cong 2 \times 1 \pmod 3 \\ &\cong 2 \pmod 3 \end{aligned}$$

$$\begin{aligned} 12 + 1234567890 \mod 10 &\cong 2 + 0 \mod 10 \\ &= 2 \mod 10 \end{aligned}$$

□

6.50

Compute $2^{1000} \% 11$

Solution.

$$\begin{aligned} 2^{10} &\cong 1 \mod 11 \\ (2^{10})^{100} &\cong 1^{100} \mod 11 \\ 2^{1000} &\cong 1 \mod 11 \end{aligned}$$

□

6.57

From the definition, find $\varphi(36)$, $\varphi(18)$, and $\varphi(28)$.

Solution.

$$\begin{aligned} \varphi(36) &= 12 \\ \varphi(18) &= 6 \\ \varphi(28) &= 12 \end{aligned}$$

□

6.52

Find the multiplicative inverse of 3 modulo 100

Solution.

$$3 \times 67 \cong 1 \mod 100.$$

□

6.80

Show that $x^2 - y^2 = 102$ has no solution in the integers.

Solution.

□

6.81

Show that $x^3 + y^3 = 3$ has no solution in the integers.

Solution.

Since $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ and 3 is prime, one of the following two cases would have to be true

1. $x + y = 1$ and $x^2 - xy + y^2 = 3$
2. $x + y = 3$ and $x^2 - xy + y^2 = 1$

Suppose the first case. Then $y = 1 - x$ so

$$\begin{aligned}x^2 - xy + y^2 = 3 &\Rightarrow x^2 - x(1 - x) + (1 - x)^2 = 3 \\&\Rightarrow 3x^2 - 3x - 2 = 0 \\&\Rightarrow x = \frac{3}{2} \text{ or } x = \frac{-1}{2}.\end{aligned}$$

In both of these two solutions, x is not an integer, so case 1 fails. Suppose instead that it is case 2. Then similarly $y = 3 - x$

$$\begin{aligned}x^2 - xy + y^2 = 1 &\Rightarrow x^2 - x(3 - x) + (3 - x)^2 = 1 \\&\Rightarrow 3x^2 - 9x + 8 = 0\end{aligned}$$

which has discriminant -15 , and so has no real solution. In both cases, we are unable to get integer solutions. Thus the equation has no integer solutions. \square

8.17

Show that

$$123456789123456789 + 234567891234567891 \neq 358025680358025680$$

Solution.

$$123456789123456789 + 234567891234567891 = 358024680358024680$$

and

$$358024680358024680 \neq 358025680358025680$$

\square