Assignment 3

Evan Curry Wilbur

March 16, 2023

5.01

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

Solution.
$1+1+1+1+1=1$. $\square$

5.02

Compute

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

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

Solution.

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

$\square$

5.03

Compute $\left(1+x+x^2\right)^4$ 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

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

$\square$

5.04

Compute the product $\left(x^4+x^3+x^2+x+1\right)\left(x^4+x+1\right)\left(x^4+x^3+1\right)$ 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:

$$x^{12}+2x^{11}+2x^{10}+3x^9+6x^8+6x^7+5x^6+6x^5+6x^4+3x^3+2x^2+2x+1$$

□

5.05

Let $g(x)=x^3+x+1$ be a generating polynomial for a CRC. Figure out how to be a little clever in computing the CRC for the bytes

111000110101000110011110

so that you don't fill up a whole sheet of paper with an enormously long division.

Solution.
content... □

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.

$$-1000 \cong 56 \mod 88.$$

□

6.07

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

Solution.
Let $r \cong N \mod m$ 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. □

6.22

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

Solution.

□

6.37

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

Solution.
content... □

6.49

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

Solution.
content... □

6.50

Compute $2^{1000}\%11$

Solution.

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

□

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

????? Check with trevor that this is the correct problem. Waiting for reply

Solution.
content... □

6.80

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

Solution.
content... □

6.81

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

Solution.
content... □

8.17

Show that

$$123456789123456789 + 234567891234567891 \neq 358025680358025680$$

Solution.
content... $\square$