Q1 Polynomials: roots

5 Points

Your answer to the blanks should be an integer, with no whitespace.

Q1.1

1 Point

True/False: For modular arithmetic modulo a prime p, $ab \equiv 0 \pmod{p}$ if and only if $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

- (●) True
- ( ) False

Explanation

If: whichever of a or b is equivalent to 0, multiplying by the other factor keeps the product equivalent to 0.

Only if: the contrapositive says that if $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$, then $ab \not\equiv 0 \pmod{p}$. This is true because p is prime and not in the factorization of a or b.

Q1.2

1 Point

If $p(x)$ has a root at $x = 4$, what is the value of $p(4)$?

0

Explanation

This is the definition of a root.

Q1.3
1 Point

If $p(x) = (x-2)(x+3)$ over the reals, what is the largest root?

2

Explanation

$p(2) = 0$. The only other root is $x = -3$.

Q1.4
1 Point

What is the maximum number of roots of a polynomial of degree d over arithmetic modulo a prime p?

- ○ 1
- ○ d - 1
- ◉ d
- ○ d + 1

Explanation

This is Property 1 from the notes, which is proven for polynomials over any field.

Q1.5
1 Point

4 is a root of the polynomial $(x+1)(x-3) \pmod 5$.

- ◉ True
- ○ False

Explanation

We have that -1 is a root because of the term $x+1$, and $-1 \equiv 4 \pmod 5$.

Q2 Interpolation

3 Points

Consider a polynomial $p(x) = a_1 x + a_0$ where $p(0) = 1$ and $p(1) = 5$.

Your answers to the following subparts should be an integer, with no whitespace.

Q2.1

1 Point

What is a_0?

1

Explanation

See explanation of 2.3

Q2.2

1 Point

What is a_1?

4

Explanation

See explanation of 2.3

Q2.3
1 Point

What is $p(2)$?

9

Explanation

$a_0 = 1$ and $a_1 = 4$ by solving the system $\begin{cases} 1 = a_1(0) + a_0 \\ 5 = a_1(1) + a_0 \end{cases}$. Then plug in $x = 2$ into the expression $p(x) = 4x + 1$.

Q3 Lots of Polynomials
1 Point

How many polynomials modulo 5 of degree at most 1 are there such that $p(1) = 0$?

5

Explanation

Any two points determine a degree 1 polynomial. We have chosen one point, $(1, 0)$. We could pick another x value, say, 0, and have 5 choices for its y value, i.e. 5 choices for $(0, y)$, which together with $(1, 0)$ determine a unique degree at most 1 polynomial.