

Algebra & Number Theory
MathTLC
HW #4: due Thursday, July 30

1. An unknown polynomial $a(x)$ has the following properties: $a(1) = 4$ and $a(-1) = 2$. Find the remainder when $a(x)$ is divided by $x^2 - 1$. (Hint: what can you say about the degree of the remainder?)
2. Let a and b be positive integers, and let

$$S = \{ax + by : a, b \text{ are positive integers and } ax + by > 0\}$$

- (a) Show S is nonempty by giving an element of S .
- (b) Why does S have a smallest element?

Now let $d = au + bv$ be the smallest element of S .

- (c) Explain why if $e|a$ and $e|b$, then $e|d$.
- (d) Let's show that $d|a$. By the Division Algorithm we can write $a = dq + r$ where $0 \leq r < a$.
 - i. Show that $r = a(1 - uq) + b(-vq)$.
 - ii. Explain why r can't be an element of S
 - iii. Explain why r must be 0, and that $d|a$.

A similar argument shows that $d|b$. So we've shown that the smallest element, d , of S is the greatest common divisor of a and b .

3. In problem 2, you showed that the greatest common divisor of a and b is an integer of the form $ax + by$. Use this to show that if a and b are relatively prime (i.e. $\gcd(a, b) = 1$) and $a|bc$, then $a|c$.
4. Find the quotient and remainder in $\mathbb{Z}[i]$ of $12 + 7i$ divided by $3 + 4i$.
5. This problem concerns \mathbb{Z}_p where p is a prime. Fermat's Little Theorem states that $x^p = x$ for all $x \in \mathbb{Z}_p$.
 - (a) Explain why if $x \neq 0$, then $x^{p-1} = 1$ in \mathbb{Z}_p .
 - (b) Use (a), to show that if for each integer n , $x^n = x^r$ in \mathbb{Z}_p where r is the remainder when n is divided by $p - 1$.
 - (c) Use (b) to compute $3^{11001111103}$ in \mathbb{Z}_{11} .