

HOMEWORK 2
Math 104 - Dr. Evans
UCSD Winter 2004
Due Thursday, January 15, 5:00pm

For questions 1 and 2, let $R = \mathbb{Z}[\sqrt{-5}]$, $a = 3$, and $b = 2 + \sqrt{-5}$.

1. Prove that in R , a and b have gcd equal to 1. Then show that no linear combination of a and b over R can ever equal 1. A linear combination over R means that there are integers c, d, e, f such that

$$(c + d\sqrt{-5}) \cdot 3 + (e + f\sqrt{-5}) \cdot (2 + \sqrt{-5}).$$

2. Give (with proof) an example of an element $\alpha = c + d\sqrt{-5}$ in R which is divisible by each of the “primes” a and b , but which is not divisible by the product ab .
3. Reduce the numbers 111, 1234, and 123454321 modulo 11.
4. Solve the linear congruence $5x \equiv 1 \pmod{13}$.
5. Find all solutions to the equation $x^2 \equiv x \pmod{10}$.
6. Prove that there are no solution to the equation $3x \equiv 2 \pmod{15}$.
7. (a) Prove from the definition of congruence that if $a \equiv b \pmod{n}$, then $a \cdot c \equiv b \cdot c \pmod{n}$.
(b) Give an example with $a, b, c \not\equiv 0 \pmod{n}$ such that $a \cdot c \equiv b \cdot c \pmod{n}$ but $a \not\equiv b \pmod{n}$.
8. (a) Prove from the definition of congruence that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \cdot c \equiv b \cdot d \pmod{n}$.
(b) Use part (a) and induction to prove that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \geq 1$.