

SOLUTIONS TO HOMEWORK 2
Math 104 - Dr. Evans
UCSD Winter 2004

1. Prove that in $\mathbb{Z}[\sqrt{-5}]$, $a = 3$ and $b = 2 + \sqrt{-5}$ have gcd equal to 1. Then show that no linear combination of a and b over $\mathbb{Z}[\sqrt{-5}]$ can ever equal 1. A linear combination over R means that there are integers c, d, e, f such that

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

We proved that 3 is a prime in $\mathbb{Z}[\sqrt{-5}]$ last week, so the divisors of 3 are $\{\pm 1, \pm 3\}$. Likewise, $2 + \sqrt{-5}$ is a prime in $\mathbb{Z}[\sqrt{-5}]$ by a similar argument, so the divisors of $2 + \sqrt{-5}$ are $\{\pm 1, \pm(2 + \sqrt{-5})\}$. Hence, the common divisors of 3 and $2 + \sqrt{-5}$ are $\{\pm 1\}$. Alternatively, one could argue that $\pm 3 \nmid 2 + \sqrt{-5}$, and so the only common divisors are $\{\pm 1\}$.

To show that $d = 1$ is a greatest common divisor of 3 and $2 + \sqrt{-5}$, we must check the two conditions stated in class. Clearly d is a divisor of both 3 and $2 + \sqrt{-5}$. Also, every common divisor (namely, ± 1) is a divisor of d for obvious reasons ($d = 1 \cdot 1 = -1 \cdot -1$). Hence, $d = 1$ is a greatest common divisor.

We now show that no linear combination of 3 and $2 + \sqrt{-5}$ equals 1 over $\mathbb{Z}[\sqrt{-5}]$. Suppose that there was such a linear combination. Then there exist integers c, d, e, f such that

$$(c + d\sqrt{-5}) \cdot 3 + (e + f\sqrt{-5}) \cdot (2 + \sqrt{-5}) = 1$$

Expanding and gathering real and imaginary parts together, we have

$$(3c + 2e - 5f) + (3d + e + 2f)\sqrt{-5} = 1 + 0\sqrt{-5}$$

Hence, we have two equations and four unknowns:

$$3c + 2e - 5f = 1$$

$$3d + e + 2f = 0$$

Adding the two equations together results in

$$3c + 3d + 3e - 3f = 3(c + d + e - f) = 1$$

Since all unknowns must be integers, 3 divides the left hand side of the equation but not the right hand side. This is a contradiction, so no such linear combination over $\mathbb{Z}[\sqrt{-5}]$ exists.

Alternatively, one could reduce the equations modulo 3 first to get

$$2e + f \equiv 1 \pmod{3}$$

$$e + 2f \equiv 0 \pmod{3}$$

Adding the two equations together, we have

$$3e + 3f \equiv 1 \pmod{3}$$

which leads to a contradiction, since $3e + 3f \equiv 0 \pmod{3}$ for any integers e, f .

2. Give (with proof) an example of an element $\alpha = c + d\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ which is divisible by each of the "primes" $a = 3$ and $b = 2 + \sqrt{-5}$, but which is not divisible by the product ab .

There are many correct answers, but here is one presented as an example in class several times. Let $\alpha = 9$. Then in $\mathbb{Z}[\sqrt{-5}]$, $3|9$ since $9 = 3 \cdot 3$. Likewise, $2 + \sqrt{-5}|9$ since $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. However, the product $3(2 + \sqrt{-5}) \nmid 9$. To see this, divide by 3 on both sides to get $(2 + \sqrt{-5}) \nmid 3$, which follows from last week's homework that 3 is prime in $\mathbb{Z}[\sqrt{-5}]$.

3. Reduce the numbers 111, 1234, and 123454321 modulo 11.

$111 - 10 \cdot 11 = 1$, so by the definition of congruence, $111 \equiv 1 \pmod{11}$. One can try to find the largest multiple of 11 less than the other two numbers and subtract, but this get exceedingly difficult. Instead, we'll use a trick shown in class for reducing modulo 11. The trick is based on the fact that $10 \equiv -1 \pmod{11}$. Hence, $10^k \equiv (-1)^k \pmod{11}$, which is 1 if k is even and -1 if k is odd.

Here's how to apply the trick for 1234. Begin by splitting 1234 into its digits times powers of 10:

$$1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$$

Now reduce modulo 11:

$$1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0 \equiv 1 \cdot (-1) + 2 \cdot (1) + 3 \cdot (-1) + 4 \cdot 1 \pmod{11}$$

This reduces to alternating adding and subtracting the digits from one another, starting with adding the ones digits. This gives us the desired answer:

$$1234 \equiv -1 + 2 - 3 + 4 \equiv 2 \pmod{11}$$

For 123454321, we'll just apply the trick without going through all the justification (which is perfectly fine for your answers).

$$123454321 \equiv 1 - 2 + 3 - 4 + 5 - 4 + 3 - 2 + 1 \equiv 1 \pmod{11}$$

4. Solve the linear congruence $5x \equiv 1 \pmod{13}$.

13 is pretty small, so one way to solve this equation is by plugging in all the numbers between 0 and 12 for x until one works.

$5 \cdot 0 \equiv 0 \not\equiv 1 \pmod{13}$	$5 \cdot 7 \equiv 9 \not\equiv 1 \pmod{13}$
$5 \cdot 1 \equiv 5 \not\equiv 1 \pmod{13}$	$5 \cdot 8 \equiv 1 \equiv 1 \pmod{13}$
$5 \cdot 2 \equiv 10 \not\equiv 1 \pmod{13}$	$5 \cdot 9 \equiv 6 \not\equiv 1 \pmod{13}$
$5 \cdot 3 \equiv 2 \not\equiv 1 \pmod{13}$	$5 \cdot 10 \equiv 11 \not\equiv 1 \pmod{13}$
$5 \cdot 4 \equiv 7 \not\equiv 1 \pmod{13}$	$5 \cdot 11 \equiv 3 \not\equiv 1 \pmod{13}$
$5 \cdot 5 \equiv 12 \not\equiv 1 \pmod{13}$	$5 \cdot 12 \equiv 8 \not\equiv 1 \pmod{13}$
$5 \cdot 6 \equiv 4 \not\equiv 1 \pmod{13}$	

Hence, the solution is $x \equiv 8 \pmod{13}$. $x = 8 + 13k$ for any integer k is also an acceptable answer.

5. Find all solutions to the equation $x^2 \equiv x \pmod{10}$.

Again, 10 is small enough to check all possible values between 0 and 9.

$0^2 = 0 \equiv 0 \pmod{10}$	$5^2 = 25 \equiv 5 \pmod{10}$
$1^2 = 1 \equiv 1 \pmod{10}$	$6^2 = 36 \equiv 6 \pmod{10}$
$2^2 = 4 \not\equiv 2 \pmod{10}$	$7^2 = 49 \not\equiv 7 \pmod{10}$
$3^2 = 9 \not\equiv 3 \pmod{10}$	$8^2 = 64 \not\equiv 8 \pmod{10}$
$4^2 = 16 \not\equiv 4 \pmod{10}$	$9^2 = 81 \not\equiv 9 \pmod{10}$

Hence, the solutions to $x^2 \equiv x \pmod{10}$ are $x \equiv 0, 1, 5, 6 \pmod{10}$.

6. Prove that there are no solution to the equation $3x \equiv 2 \pmod{15}$.

Assume there is a solution for x . Then by the definition of congruence, there exists an integer k such that $3x = 2 + 15k$. Subtracting $15k$ on both sides and factoring out 3, we have $3(x - 5k) = 2$. Now 3 divides $3(x - 5k)$, but 3 does not divide 2. This is a contradiction, hence no such solution for x exists.

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 $a \not\equiv b \pmod{n}$.

(a) Suppose $a \equiv b \pmod{n}$. By definition, there exists an integer k such that $a = b + kn$. Multiplying by c on both sides, we have $ac = bc + (ck)n$. Since ac and bc differ by an integer multiple of n , $ac \equiv bc \pmod{n}$.

(b) There are many correct answers. However, every correct answer must have n be a composite number. The simplest example is $n = 4$, $a = 1$, $b = 3$, and $c = 2$. Then $1 \not\equiv 3 \pmod{4}$, but $1 \cdot 2 \equiv 3 \cdot 2 \pmod{4}$.

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 $k \geq 1$.

(a) Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition, there exist integers k and l such that $a = b + kn$ and $c = d + ln$. Multiplying the equations together results in

$$\begin{aligned} ac &= (b + kn)(d + ln) \\ &= bd + knd + bln + kln^2 \\ &= bd + n(kd + bl + kln) \end{aligned}$$

Since ac and bd differ by an integer multiple of n , $ac \equiv bd \pmod{n}$.

(b) Base Case The equation holds true for $k = 1$, since $a^1 \equiv b^1 \pmod{n}$ by assumption.

Inductive Step Assume the equation is true for k , that is, $a^k \equiv b^k \pmod{n}$. By assumption, $a \equiv b \pmod{n}$. By part (a), $a^k \cdot a \equiv b^k \cdot b \pmod{n}$, or $a^{k+1} \equiv b^{k+1} \pmod{n}$. Hence, the equation holds true for $k + 1$.

By the principle of mathematical induction, $a^k \equiv b^k \pmod{n}$ for all $k \geq 1$.