Solutions to Homework for M351 – Algebra I

Hwk 42:

In the ring $\mathbb{Z}[i]$, find a greatest common divisor of $a = 16 + 2i$ and $b = 14 + 31i$, using repeated division with remainder in analogy to Problem 25.

(Note that I said: **a** GCD, with the indefinite article. If g is a GCD, then $-g$, ig and $-ig$ also are correct solutions. The option of selecting 'the positive one' is not available here.)

Solution:

$\frac{16+2i}{14+31i} = \frac{286-468i}{1157}$ rounds to 0 $\qquad 16 + 2i = (0 + 0i)(14 + 31i) + (16 + 2i)$

$\frac{14+31i}{16+2i} = \frac{286+468i}{260}$ rounds to $1 + 2i$ $\qquad 14 + 31i = (1 + 2i)(16 + 2i) + (2 - 3i)$

$\frac{16+2i}{2-3i} = \frac{26+52i}{13} = 2 + 4i$ no remainder $\qquad 16 + 2i = (2 + 4i)(2 - 3i) + 0$

So $2 - 3i$ is a gcd of $16 + 2i$ and $14 + 31i$. (The other gcd's are $-2 + 3i$, $2i + 3$, $-2i - 3$.)

Hwk 43:

Give the isomorphism $\theta : \mathbb{Z}_{12} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4$ afforded by the chinese remainder theorem explicitly (i.e., table all values). — Likewise for $\theta : \mathbb{Z}_{10} \to \mathbb{Z}_2 \oplus \mathbb{Z}_5$.

Also show that there cannot be an isomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$. To do this, observe, for instance, the number of solutions to the equation $x + x = 0$ in either ring. Come up with at least one other equation (using multiplication) that has different numbers of solutions in either ring. (Doing so amounts to giving a second proof that there cannot be an isomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$). Include a formally sufficient proof of the last statement in the following note, such as to make rigorous why the number of solutions to an equation involving only ring operations can be used to show that two rings are not isomorphic.

Note: How would one typically show that two rings are isomorphic? Easy in principle: one exhibts a mapping explicitly and shows that it is 1-1, onto, and a homomorphism. This does not mean that the task is always easy in practice. — But how does one show that two rings are NOT *isomorphic? Not so easy in principle. One has to show that no 1-1 onto map watsoever can be a homomorphism. Between two rings with just four lousy elements, there would be 24 bijective maps already to check for homomorphism properties. This problem shows a more feasible approach: Find properties that are preserved under isomorphisms: If a certain equation in one ring R has exactly n solutions $x_1, \ldots, x_n$, then it has exactly n solutions in any other ring S that is isomorphic to R; if $\theta : R \to S$ is a ring isomorphism, then the solutions to that equation in S are $\theta(x_1), \ldots, \theta(x_n)$.*

Solution :

θ :
$\bar{0}_{12} \mapsto (\bar{0}_3, \bar{0}_4)$
$\bar{1}_{12} \mapsto (\bar{1}_3, \bar{1}_4)$
$\bar{2}_{12} \mapsto (\bar{2}_3, \bar{2}_4)$
$\bar{3}_{12} \mapsto (\bar{0}_3, \bar{3}_4)$
$\bar{4}_{12} \mapsto (\bar{1}_3, \bar{0}_4)$
$\bar{5}_{12} \mapsto (\bar{2}_3, \bar{1}_4)$
$\bar{6}_{12} \mapsto (\bar{0}_3, \bar{2}_4)$
$\bar{7}_{12} \mapsto (\bar{1}_3, \bar{3}_4)$
$\bar{8}_{12} \mapsto (\bar{2}_3, \bar{0}_4)$
$\bar{9}_{12} \mapsto (\bar{0}_3, \bar{1}_4)$
$\bar{10}_{12} \mapsto (\bar{1}_3, \bar{2}_4)$
$\bar{11}_{12} \mapsto (\bar{2}_3, \bar{3}_4)$

θ :
$\bar{0}_{10} \mapsto (\bar{0}_2, \bar{0}_5)$
$\bar{1}_{10} \mapsto (\bar{1}_2, \bar{1}_5)$
$\bar{2}_{10} \mapsto (\bar{0}_2, \bar{2}_5)$
$\bar{3}_{10} \mapsto (\bar{1}_2, \bar{3}_5)$
$\bar{4}_{10} \mapsto (\bar{0}_2, \bar{4}_5)$
$\bar{5}_{10} \mapsto (\bar{1}_2, \bar{0}_5)$
$\bar{6}_{10} \mapsto (\bar{0}_2, \bar{1}_5)$
$\bar{7}_{10} \mapsto (\bar{1}_2, \bar{2}_5)$
$\bar{8}_{10} \mapsto (\bar{0}_2, \bar{3}_5)$
$\bar{9}_{10} \mapsto (\bar{1}_2, \bar{4}_5)$

By testing all elements, $\bar{0}_4$, $\bar{1}_4$, $\bar{2}_4$, $\bar{3}_4$, we see that $x + x = 0$ has two solutions in $\mathbb{Z}_4$, namely $x = \bar{0}_4$ or $x = \bar{2}_4$. In $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ all four elements $(\bar{0}_2, \bar{0}_2)$, $(\bar{0}_2, \bar{1}_2)$, $(\bar{1}_2, \bar{0}_2)$, $(\bar{1}_2, \bar{1}_2)$ solve the equation $x + x = 0$.

If $\theta : R \to S$ is a ring homorphism and x satisfies the equation $x + x = 0$ in R, then $\theta(x) + \theta(x) = \theta(x + x) = \theta(0) = 0$. So $y = \theta(x)$ satisfies the equation $y + y = 0$ in the ring S. If θ is 1-1, then to different solutions x in R, one gets different solutions $y = \theta(x)$ in S. If θ is also onto, then every y is of the form $y = \theta(x)$ for some x. Now if y solves $y + y = 0$, then $\theta(x + x) = \theta(0)$ by the above calculation; since θ is 1-1, we can again conclude that x solves $x + x = 0$. So there is a bijective correspondence between solutions of $x + x = 0$ in R and solutions to the same equation $y + y = 0$ in S.

Here is another equation that does the trick: $x \cdot x = 0$ has two solutions $\bar{0}_4$ and $\bar{2}_4$ in $\mathbb{Z}_4$, but only one solution $(\bar{0}_2, \bar{0}_2)$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Or, another example, the equation $x \cdot x = x$ has two solutions in $\mathbb{Z}_4$, but four solutions in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. The equation $x \cdot x = 1$ has two solutions in $\mathbb{Z}_4$, but only one solution in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Hwk 44:

Use modular arithmetic to show that the following determinant is not 0:

$$\begin{vmatrix} 1 & 3 & 5 & 0 & 2 & 4 \\ 5 & 2 & 1 & 2 & 4 & 2 \\ 10 & 5 & 3 & 7 & 1 & 0 \\ -5 & 5 & 15 & 11 & -7 & 10 \\ 15 & 0 & -5 & 20 & 5 & 3 \\ 0 & -10 & 5 & 10 & 3 & 5 \end{vmatrix}$$

Solution: The determinant of a matrix is a certain polynomial in the entries of that matrix, according to the formula $\det A = \sum_\pi \text{sign}\pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$ where, in our example, the size of the matrix, $n = 6$. The sum extends over all permutations $\pi \in S_n$. With the entries in $\mathbb{Z}$, the determinant can be seen as a calculation within that ring. We may reduce modulo some number a: For matrices A, B: If $A \equiv B \bmod a$ (componentwise), then $\det A \equiv \det B \bmod a$ We use this with $a = 5$, to create many zeros in the modular arithmetic determinant: entries $*$ denote numbers we don't bother to calculate because they are not relevant.

$$\begin{vmatrix} 1 & 3 & 5 & 0 & 2 & 4 \\ 5 & 2 & 1 & 2 & 4 & 2 \\ 10 & 5 & 3 & 7 & 1 & 0 \\ -5 & 5 & 15 & 11 & -7 & 10 \\ 15 & 0 & -5 & 20 & 5 & 3 \\ 0 & -10 & 5 & 10 & 3 & 5 \end{vmatrix} \equiv \begin{vmatrix} 1 & * & * & * & * & * \\ 0 & 2 & * & * & * & * \\ 0 & 0 & 3 & * & * & * \\ 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 0 \end{vmatrix} = -1 \cdot 2 \cdot 3 \cdot 1 \cdot 3 \cdot 3 = -54 \equiv 1 \bmod 5$$

So since the determinant is congruent 1 mod 5, it cannot be 0.

Hwk 45:

How many zeros exactly are at the end of the decimal representation of the number 93!, written out in digits? Only count the contingent zeros at the end, after the last non-zero digits. For instance, for the number 350102100000, you would count five zeros.

Solution: Notation: $\lfloor x \rfloor$ denotes the largest integer $\leq x$.

The number of trailing zeros is the largest n such that 10^n divides 93!. In the prime factor decomposition, 93! has the prime 5 to the power 21. Namely, the factors $5, 10, 15, \dots, 90$ contribute

each (at least) a factor 5 to the product $1\cdot 2\cdot 3\cdot 4\cdot 5\cdots 89\cdot 90\cdot 91\cdot 92\cdot 93$. This makes $\lfloor \frac{93}{5} \rfloor = 18$ many terms already. However, the multiples of $25 = 5^2$ actually contribute a second factor of 5 (not counted yet) to the product, which makes another three occurrences.

Likewise, the number of factors 2 in 93! is $\lfloor \frac{93}{2} \rfloor + \lfloor \frac{93}{4} \rfloor + \lfloor \frac{93}{8} \rfloor + \lfloor \frac{93}{16} \rfloor + \lfloor \frac{93}{32} \rfloor + \ldots = 46 + 23 + 11 + 5 + 2 + 1 = 88$. This is of course larger than the number of factors 5. So the number of trailing zeros in 93! is 21.

Hwk 46:

> Find all numbers n such that $\varphi(n) = 12$. Show that there are no numbers n such that $\varphi(n) = 14$.

Solution: If we write n in the form of the prime number decomposition, $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, then $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1)$. This implies: If p is a prime number divinding n, then $p-1$ must divide $\varphi(n)$. If a higher power of p divides n, then p must also divide n. We can therefore analyze the possible prime factors of n by looking at the divisors of $\varphi(n)$.

If $\varphi(n) = 12$, we look at the divisors of 12: They are: 1,2,3,4,6,12. Any prime divisors p of n must therefore be found among: 2,3,4,5,7,13 (we added 1 to each divisor of $\varphi(n) = 12$). Of course 4 is not a prime, so n can contain at most the primes $2, 3, 5, 7, 13$.

2 can show up at most with power 3 in the prime factorization of n, since $\varphi(2^3) = 2^2(2-1) = 4$ still divides 12, but $\varphi(2^4) = 2^3(2-1) = 8$ does not divide 12 any more. Likewise, 3 can show up at most with power 2. All the other prime factors cannot show up with a higher power at all.

Case 1: 13 divides n. Let $n = 13m$. m will be relative prime to 13, because we know that 13^2 cannot divide n. Since $\varphi(13) = 12$, we must have $\varphi(m) = 1$. So m can have no other prime fuctors but 2, and we have $m = 1$ or $m = 2$. This gives us two solutions: $n \in \{13, 26\}$.

Case 2 13 doesn't divide n, but 7 divides n. So let $n = 7m$. Again $gcd(7, m) = 1$. We need $\varphi(m) = 2$. By the same divisor argument m can have only 2 and 3 as prime factors, and we only have two choices: m is either 3, 4 or 6. This gives us two further solutions: $n \in \{21, 28, 42\}$.

Case 3: Neither 13 nor 7 divide n. If $n = 5m$, we need $12 = \varphi(5)\varphi(m)$. Hence $\varphi(m) = 3$. But there is no such m: Actually $\varphi(m)$ is never an odd number other than 1. For, whenever m contains an odd prime factor, then $\varphi(m)$ must be even, due to the $(p-1)$ factor. But is m is a power of 2, we again get an even $\varphi(m)$, from $p^{\alpha-1}$, unless $m = 1$ or $m = 2$. In these cases however $\varphi(m) = 1$. No solution here.

We harvest for later use: $\varphi(m)$ will never be an odd number other than 1.

Case 4: $n = 2^a 3^b$ with $a \leq 3$ and $b \leq 2$. The only choice here for $\varphi(n) = 12$ is $n = 2^2 \cdot 3^2 = 36$.

We have found altogether six solutions n to $\varphi(n) = 12$. Namely, $n \in \{13, 21, 26, 28, 36, 42\}$.

Now study $\varphi(n) = 14$. The divisors of 14 are 1,2,7,14. So the prime factors of n must be found among 2,3,8,15. But only 2,3 are prime. But $\varphi(2^a 3^b)$ could not contain a prime factor 7. Therefore $\varphi(n) = 14$ cannot happen for any n.

Hwk 47:

> Let's try the ring $\mathbb{Z}[\sqrt{-5}]$ for a change: another subring of $\mathbb{C}$; it consists of all the numbers $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.
>
> First show that the only numbers dividing the identity 1 in this ring are $+1$ and -1: you have to find all integers a, b, c, d such that $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$.
>
> Now show that 3 has no divisors but ± 3 and ± 1 in this ring. Show the analog for the numbers 2 and $1 \pm \sqrt{-5}$. In other words, all of these numbers are irreducible in the ring

$\mathbb{Z}[\sqrt{-5}]$. (Remember: irreducible means that the number cannot be factored further except by introducing units (= divisors of 1) as factors.)

Hint: The task to find all integers a, b, c, d such that $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$ (or 3 etc) is simplified a lot if you first multiply this equation with its complex conjugate.

Solution: A unit $A \in \mathbb{Z}[\sqrt{-5}]$ is an A such that there exists $C \in \mathbb{Z}[\sqrt{-5}]$, where $AC = 1$. So suppose $A = a + b\sqrt{-5}$ is a unit and $C = c + d\sqrt{-5}$ is such that $AC = 1$. By taking the complex conjugate, we conclude $\bar{A}\bar{C} = 1$. Multiplying the two, we get $(a^2 + 5b^2)(c^2 + 5d^2) = 1^2 = 1$. The two factors are integers of course, so $a^2 + 5b^2$ must divide 1. The only divisors of 1 are ± 1, but $a^2 + 5b^2 \geq 0$. Hence $a^2 + 5b^2 = 1$ This can only happen if $b = 0$ and $a = \pm 1$.

There is another method to prove the same thing: If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$, then $ac-5bd = 1$ and $ad + bc = 0$. We want to show $bd = 0$ first, and we do it by ruling out the possibilities $bd > 0$ and $bd < 0$. Clearly, if $bd > 0$, then $ac = 1 + 5bd > 0$, and therefore $(ad)(bc) = (ac)(bd) > 0$. But if ad and bc have the same sign, their sum cannot be 0. On the other hand, if $bd < 0$, then (being an integer) $bd \leq -1$; hence $ac = 1 + 5bd \leq -4 < 0$. Again we conclude that ad and bc have the same sign, making $ac + bd = 0$ impossible. — Now that we know $bd = 0$, we conclude $ac = 1$, so $a = c = \pm 1$. With this plugged in, $ad + bc = 0$ implies $b + d = 0$. With $bd = 0$, we conclude $b = d = 0$.

If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 3$, multiplication with the complex conjugate gives $(a^2+5b^2)(c^2+5d^2) = 9$. So $(a^2 + 5b^2)$ must divide 9, hence (being nonnegative) it can only be 1, 3, or 9. In particular $|a| \leq 3$ and $|b| < 2$. Inspecting all case, we see that the only integer solutions to $a^2+5b^2 \in \{1; 3; 9\}$ are $a+b\sqrt{-5} \in \{\pm 1; ; \pm 3, \pm 2 \pm \sqrt{-5}\}$ with $c+d\sqrt{-5} \in \{\pm 3, \pm 2 \pm \sqrt{-5}; ; \pm 1\}$ respectively. However, the last cases do not give rise to divisors of 3 since $(\pm 2 \pm \sqrt{-5})(\pm 1) \neq 3$. (Of course when taking $|\cdot|^2$ of the equation, we found a necessary, but not sufficient, condition.)

If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 2$, multiplication with the complex conjugate gives $(a^2+5b^2)(c^2+5d^2) = 4$. So $(a^2 + 5b^2)$ must divide 4, hence (being nonnegative) it can only be 1, 2, or 4. In particular $|a| \leq 2$ and $b = 0$. Likewise $d = 0$. But then the factors must be integers, and the only factorization of 2 within $\mathbb{Z}$ is $2 \cdot 1$ of $(-2)(-1)$.

Now $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1+\sqrt{-5}$, implies $(a^2+5b^2)(c^2+5d^2) = 6$, hence $a^2+5b^2 \in \{1, 2, 3, 6\}$. 2 and 3 cannot occur as values of $a^2 + 5b^2$; in the other two cases, we obtain $a = \pm 1$. Then $b = 0$ or $b = \pm 1$ respectively. — Same argument for $1 - \sqrt{-5}$.

Hwk 48:

Show that in the ring $\mathbb{Z}[\sqrt{-5}]$, the number 6 can be written as a product of irreducible factors in two essentially different ways. (Refer to previous problem for raw material).

Solution: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Since each of the four numbers in the factorization is different from ± 1 times any other among the four numbers (± 1 being the only units), the two factorizations are essentially different.

Hwk 49:

Given a commutative ring R with identity, we consider the set $\mathrm{Seq}(R)$ consisting of all sequences $s = (s_0, s_1, s_2, s_3, \ldots)$ where each s_i is an element of R. For instance, with $R = \mathbb{Z}$, the following are elements of $\mathrm{Seq}(\mathbb{Z})$: $(0, 1, 4, 9, \ldots)$, or $(1, 0, -1, 0, 1, 0, -1, \ldots)$. Generally, we will denote by s_i the i^{th} entry in the sequence s, where we begin to count entries at number 0. We define the following operations on $\mathrm{Seq}(R)$:

The *sum* $a+b$ of two sequences is defined componentwise: $a+b = (a_0+b_0, a_1+b_1, a_2+b_2, \ldots)$. The Cauchy product of two sequences is defined as follows:

$$ab = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots)$$

such that $(ab)_n = \sum_{i=0}^n a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0$.

(a) Make sure that you understand the definition: To this end, calculate the Cauchy product ab of the sequence $a = (1, 1, 1, 1, 1, 1, \ldots)$ with $b = (0, 1, 2, 3, 4, 5, \ldots)$ in $\mathrm{Seq}(\mathbb{Z})$. Which number is the the entry $(ab)_{30}$?

(b) Now show that $\mathrm{Seq}(R)$ with these operations is a commutative ring.

We call this ring $R[[X]]$ (The ad-hoc name $\mathrm{Seq}(R)$ was just for the set.)

Solution: (a) $(1, 1, 1, 1, 1, 1, \ldots) \cdot (0, 1, 2, 3, 4, 5, \ldots) = (0, 1, 3, 6, 10, 15, \ldots)$. More precisely $a_i = 1$ and $b_i = i$. So $(ab)_n = \sum_{i=0}^n 1(n-i) = \sum_{j=0}^n j = n(n+1)/2$ where we have substituted $j = n - i$. In particular $(ab)_{30} = 465$.

(b) It is clear that addition is commutative and associative, and that the zero sequence $(0, 0, 0, 0, \ldots)$ is the additive neutral. The additive inverse is given by $(-a)_n = -a_n$, or, in other words the negative of $(a_0, a_1, a_2, a_3, \ldots)$ is $(-a_0, -a_1, -a_2, -a_3, \ldots)$.

Commutativity of multiplication: we again use the summation index substitution $j = n - i$. Then $(ab)_n = \sum_{i=0}^n a_i b_{n-i} = \sum_{j=0}^n a_{n-j} b_j = \sum_{j=0}^n b_j a_{n-j} = (ba)_n$ for each n. Hence $ab = ba$. The commutativity of the ring R enters here.

Distributivity: $[(a+b)c]_n = \sum_{i=0}^n (a+b)_i c_{n-i} = \sum_{i=0}^n (a_i + b_i) c_{n-i} = \sum_{i=0}^n \{a_i c_{n-i} + b_i c_{n-i}\} = \sum_{i=0}^n a_i c_{n-i} + \sum_{i=0}^n b_i c_{n-i} = (ac)_n + (bc)_n = (ac + bc)_n$.

Associativity of multiplication: This time, since it is the most complicated part, we'll be pedantic and list all properties that are used in each step, apart from associativity of $+$, which is already implicit in the $\sum$ notation.

$$[(ab)c]_n \underset{(1)}{=} \sum_{i=0}^n (ab)_i c_{n-i} \underset{(1)}{=} \sum_{i=0}^n \left(\sum_{k=0}^i a_k b_{i-k} \right) c_{n-i} \underset{(2)}{=} \sum_{i=0}^n \sum_{k=0}^i a_k b_{i-k} c_{n-i}$$

$$[a(bc)]_n \underset{(1)}{=} \sum_{k=0}^n a_k (bc)_{n-k} \underset{(1)}{=} \sum_{k=0}^n a_k \left(\sum_{j=0}^{n-k} b_j c_{n-k-j} \right) \underset{(2)}{=} \sum_{k=0}^n \sum_{j=0}^{n-k} a_k b_j c_{n-k-j}$$

(1) def' of product — (2) distributive law in R (enhanced by induction to deal with $\sum$ of more than two terms).

In the first line let's rearrange the summation in the last double sum. Note that $\sum_{i=0}^n \sum_{k=0}^i = \sum_{k=0}^n \sum_{i=k}^n$. (Each sums over all (k, i) satisfying $0 \le k \le i \le n$.) We now substitute the summation variable i for $j := i - k$, so that $\sum_{i=k}^n = \sum_{j=0}^{n-k}$. So we continue the first line:

$$\sum_{i=0}^n \sum_{k=0}^i a_k b_{i-k} c_{n-i} = \sum_{k=0}^n \sum_{i=k}^n a_k b_{i-k} c_{n-i} = \sum_{k=0}^n \sum_{j=0}^{n-k} a_k b_j c_{n-j-k}$$

and it matches the result of the secdond line, as was to be shown.

Hwk 50:

In the ring $\mathbb{Z}[[X]]$, show that the element $a = (1, 1, 1, 1, \ldots)$ is invertible and give its inverse.

Solution: The 1-element in $\mathbb{Z}[[X]]$ is $(1, 0, 0, 0, \ldots)$. We can find this by trying to find $x = (x_0, x_1, x_2, x_3, \ldots)$ such that $(a_0, a_1, a_2, a_3, \ldots)(x_0, x_1, x_2, x_3, \ldots) = (a_0, a_1, a_2, a_3, \ldots)$ for all a_i. From $a_0 x_0 = a_0$ we get $x_0 = 1$, then from $a_0 x_1 + a_1 1 = a_1$, we get $x_1 = 0$. Next from $a_0 x_2 + a_1 0 + a_2 1 = a_2$, we get $x_2 = 0$, etc. (Formally, this is of course an induction proof).

We want to find $a = (a_0, a_1, a_2, a_3, \ldots)$ such that $(1,1,1,1,\ldots)(a_0, a_1, a_2, a_3, \ldots) = (1,0,0,0,\ldots)$. From $1a_0 = 1$, we conclude $a_0 = 1$. Then from $1a_0 + 1a_1 = 0$, we conclude $a_1 = -1$. Next, from $1a_0 + 1a_1 + 1a_2 = 0$, we conclude $a_2 = 0$, and inductively now all further a_i vanish. So we were able to find an inverse of $(1,1,1,1,\ldots)$, namely $(1,-1,0,0,\ldots)$.

[Once the X notation below is established, this is of course nothing but the geometric series from calculus, in algebraic disguise: $1+x+x^2+x^3+\ldots = (1-x)^{-1}$, hence $(1+x+x^2+x^3+\ldots)^{-1} = 1-x$.]

Hwk 51:

> We consider the subset $\mathrm{Seq}_0(R)$ of $\mathrm{Seq}(R)$, consisting of those sequences that have only finitely many non-zero entries. For instance, the sequence $(1,2,0,-7,3,0,0,0,0,\ldots)$ is in $\mathrm{Seq}_0(\mathbb{Z})$. Such sequences can be written in abbreviated form as finite sequences by omitting the trailing zeros: $(1,2,0,-7,3)$. Show that $\mathrm{Seq}_0(R)$ is a subring of $\mathrm{Seq}(R)$. In particular, to gain sufficient understanding concerning the closure of multiplication, calculate the Cauchy product of $(1,2,0,-7,3)$ and $(2,-1,4)$.

Solution: The 'training calculation' is: $(1,2,0,-7,3)\cdot(2,-1,4) := (1,2,0,-7,3,0,0,0,0,\ldots)\cdot(2,-1,4,0,0,0,0,0,0,\ldots) := (2,3,2,-6,13,-31,12,0,0,0,\ldots)$

We want to show: If $a, b \in \mathrm{Seq}_0(R)$, than so are $a-b$ and ab. Now $a \in \mathrm{Seq}_0(R)$ means there exists some N such that $a_i = 0$ for $i > N$. And $b \in \mathrm{Seq}_0(R)$ means there exists some M such that $a_i = 0$ for $i > M$.

Now if $i > \max\{M, N\}$, then both a_i and b_i are 0, hence $(a-b)_i = a_i - b_i = 0$. So $a - b \in \mathrm{Seq}_0(R)$.

Moreover if $n > M + N$, then we cannot have both $i \leq N$ and $n - i \leq M$. Therefore $a_i = 0$ or $b_{n-i} = 0$ (possibly both). But this means that in the sum $(ab)_n = \sum_{i=0}^{n} a_i b_{n-i}$, each term is 0. Hence $(ab)_n = 0$ if $n > N + M$. So $ab \in \mathrm{Seq}_0(R)$.

Hwk 52:

> In the ring $\mathrm{Seq}_0(R)$, we denote the element $(0,1)$ as X. Calculate X^0, X^2, X^3 etc., and write $(1,2,0,-7,3)$ as a linear combination of powers of X.

Solution: Obviously, the problem means to assume that R is a ring with 1, as can be seen from the definition of X. X^0 is defined to be the multiplicative neutral in any ring; namely in this ring here, it is $(1,0,0,0,\ldots)$.

$X^2 = (0,1,0,0,0,\ldots)(0,1,0,0,0,\ldots) = (0,0,1,0,0,\ldots)$,
$X^3 = (0,0,1,0,0,\ldots)(0,1,0,0,0,\ldots) = (0,0,0,1,0,\ldots)$,
$X^4 = (0,0,0,1,0,\ldots)(0,1,0,0,0,\ldots) = (0,0,0,0,1,0,\ldots)$, etc.

(More formally, we prove by induction over n, that $(X^n)_j = 0$ for $j \neq n$ and $(X^n)_n = 1$.)

We can write, for instance, in the ring $\mathrm{Seq}_0(\mathbb{Z})$, from which the example is taken, $(1,2,0,-7,3) = 1X^0 + 2X^1 - 7X^3 + 3X^4$.

In a more general commutative ring R with 1, you may wonder about writing, e.g., (a_0, a_1, a_2, a_3) as $a_0X^0 + a_1X^1 + a_2X^2 + a_3X^3$. This latter expression appears to involve multiplications of elements of different rings, namely $a_i \in R$, but $X^i \in R[X]$. The way to understand this is to intend a_i as a shorthand for $(a_i, 0, 0, 0, \ldots)$. Note that the mapping $a \mapsto (a,0,0,0,\ldots)$, $R \mapsto R[X]$ is an injective ring homomorphism. This allows us to pretend that R is a subring of $R[X]$.

Hwk 53:

> From now on, we will take the liberty of writing the elements of $\mathbb{Z}_n$ as $0, 1, 2, \ldots, n-1$, rather than $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ when no confusion arises. Calculate $(1+2X)^3$ in the ring $\mathbb{Z}_3[X]$.

Solution: This is too easy: $(1+2X)^2 = (1+2X)(1+2X) = 1+4X+4X^2 = 1+X+X^2$. $(1+2X)^3 = (1+2X)(1+X+X^2) = 1+3X+3X^2+2X^3 = 1+2X^3$.

Note that the exponents are nonnegative integers, whereas the coefficients are not integers, but congruence classes, in $\mathbb{Z}_3$. You can use the binomial theorem, which is valid in every commutative ring with 1, because it relies only on these axioms. However, then, issues get swept under the carpet if you omit the overline notation for congruence classes:

$$(\bar{1}+\bar{2}X)^3 = \bar{1}^3 + 3\cdot\bar{1}^2(\bar{2}X) + 3\cdot\bar{1}(\bar{2}X)^2 + (\bar{2}X)^3 = \ldots$$

Note that in any ring, ring elements can be multiplied with integers, namely $1\cdot r = r$, $2\cdot r = r+r$, $3\cdot r = r+r+r$, etc. $(-1)r = -r$, $(-2)r = (-r)+(-r)$, etc. For the ring $\mathbb{Z}_n$, this understanding implies that $a\bar{b} = \bar{a}\bar{b}$. (The first is integer times congruence class, the second a product of congruence classes.)

$$\ldots = \bar{1} + \bar{2}^3X^3 = \bar{1} + \bar{2}X^3$$

Hwk 54:

> In the polynomial ring $\mathbb{Z}_6[X]$, find two polynomials p and q, such that $\deg(pq) < (\deg p)+(\deg q)$. Note that $\mathbb{Z}_6$ is not an integral domain; so the purpose of this problem is to show that the assumption that the coefficient ring be an integral domain is really needed for the degree formula to hold.

Solution: For instance $p = \bar{2}X + \bar{1}$ and $q = \bar{3}X + \bar{1}$. Since $\bar{2}\cdot\bar{3} = \bar{0}$, we have $pq = \bar{5}X + \bar{1}$. So $1 = \deg(pq) < \deg p + \deg q = 1+1$.

Hwk 55:

> In the ring $\mathbb{Z}[X]$ take the polynomials $a = X^3+X^2+2X+1$ and $b = 2X^2$. Show that it is not possible to find polynomials q and r in $\mathbb{Z}[X]$ such that $a = bq+r$ and $\deg r < \deg b$. If the coefficients are taken from a field, the euclidean algorithm asserts that such a division with remainder is possible. So this problem serves as an illustration that the requirement that the coefficient ring be a field is really needed for the euclidean algorithm.

Solution: If $\deg r < \deg b$, then (with $\deg bq = \deg b + \deg q \geq \deg b$) we obtain $\deg r < \deg bq$ and therefore $\deg(bq+r) = \deg bq = \deg b + \deg q$. So since $\deg a = 3$ and $\deg b = 2$, we need $\deg q = 1$. This means $q = c_0 + c_1X$. Comparing the X^3 coefficient of a and $bq+r$ (to which r doesn't contribute), we find $1 = 2c_1$ with $c_1 \in \mathbb{Z}$. This is not possible b/c 2 is not a unit in $\mathbb{Z}$.

Hwk 56:

> In the ring $\mathbb{Q}[X]$, find a GCD of $a = X^3-7X^2+3X+3$ and $b = X^3-6X^2+X+7$. Also write the GCD thus obtained as a linear combination of a and b.

Solution: Let's do a long division with $a_0 := a$ and $a_1 := b$ So we write $a_0 = q_0 a_1 + a_2$ (defining a_2 to be the remainder), and then $a_1 = q_1 a_2 + a_3$, etc.

$$\begin{array}{l|r} a_0 = q_0 a_1 + a_2 & X^3 - 7X^2 + 3X + 3 = 1 \cdot (X^3 - 6X^2 + X + 7) + (-X^2 + 2X - 4) \\ a_1 = q_1 a_2 + a_3 & X^3 - 6X^2 + X + 7 = (-X + 4) \cdot (-X^2 + 2X - 4) + (-11X + 23) \\ a_2 = q_2 a_3 + a_4 & -X^2 + 2X - 4 = (\frac{1}{11}X + \frac{1}{121}) \cdot (-11X + 23) + (-\frac{507}{121}) \\ a_3 = q_3 a_4 + a_5 & -11X + 23 = (\frac{1331}{507}X - \frac{121 \cdot 23}{507}) \cdot (-\frac{507}{121}) + 0 \end{array}$$

So we find that the constant polynomial $-\frac{507}{121}$ is a gcd of a and b. Since gcd's are determined only up to a unit in the ring (which means in $\mathbb{Q}[X]$, up to a constant polynomial), we may more conveniently answer that 1 is a gcd of a and b.

Now let's write the gcd, which is a_4, as a linear combination of a_0 and a_1. We do it successively:

$$\begin{aligned} a_4 &= a_2 - q_2 a_3 = a_2 - q_2(a_1 - q_1 a_2) = (1 + q_1 q_2)a_2 - q_2 a_1 = (1 + q_1 q_2)(a_0 - q_0 a_1) - q_2 a_1 = \\ &= (1 + q_1 q_2)a_0 + (-q_2 - q_0 - q_0 q_1 q_2)a_1 = \\ &= \tfrac{1}{121}(121 - (-X + 4)(11X + 1))a + \tfrac{1}{121}(-11X - 1 - 121 + (-X + 4)(11X + 1))b \\ -507 &= (-11X^2 + 43X + 125)a + (11X^2 - 54X - 126)b \end{aligned}$$

You might have started in reverse order, with $a_1 := a$ and $a_0 := b$. Then the calculation would have looked slightly differently, but with the same conclusion:

$$\begin{array}{l|r} a_0 = q_0 a_1 + a_2 & X^3 - 6X^2 + X + 7 = 1 \cdot (X^3 - 7X^2 + 3X + 3) + (X^2 - 2X + 4) \\ a_1 = q_1 a_2 + a_3 & X^3 - 7X^2 + 3X + 3 = (X - 5) \cdot (X^2 - 2X + 4) + (-11X + 23) \\ a_2 = q_2 a_3 + a_4 & X^2 - 2X + 4 = (-\frac{1}{11}X - \frac{1}{121}) \cdot (-11X + 23) + (\frac{507}{121}) \\ a_3 = q_3 a_4 + a_5 & -11X + 23 = (-\frac{1331}{507}X + \frac{121 \cdot 23}{507}) \cdot (\frac{507}{121}) + 0 \end{array}$$

Hwk 57:

> In the ring $\mathbb{Z}_{13}[X]$, find a GCD of the "same" polynomials $a = X^3 - 7X^2 + 3X + 3$ and $b = X^3 - 6X^2 + X + 7$, and write the GCD thus obtained as a linear combination of a and b.
>
> I put the word "same" in quotes, because this is an abuse of language. The coefficent -6 in b of problem 56 is the integer -6, whereas in problem 57, the 'same' -6 is a shorthand for the element $\overline{-6}_{13} = \overline{7}_{13} \in \mathbb{Z}_{13}$. But it's nevertheless common language usage to consider the 'same' polynomial in different rings.

Solution: In order to do the divisions in the field $\mathbb{Z}_{13}$, it is convenient to have a list of inverses at hand, and these are found by trial and error multiplications: $2 \cdot 7 = 1$, $3 \cdot 9 = 1$, $4 \cdot 10 = 1$, $5 \cdot 8 = 1$, $6 \cdot 11 = 1$, $12 \cdot 12 = 1$ in $\mathbb{Z}_{13}$. I could write standard representatives, like 6 instead of -7, but I'll stick with the given form. To reuse much of the previous calculation, note $1/11 = 6$ in the ring at hand. Remember that all the coefficients are NOT integers, but congruence classes, and the bars have simply been omitted for notational convenience.

$$\begin{array}{l|r} a_0 = q_0 a_1 + a_2 & X^3 - 7X^2 + 3X + 3 = 1 \cdot (X^3 - 6X^2 + X + 7) + (-X^2 + 2X - 4) \\ a_1 = q_1 a_2 + a_3 & X^3 - 6X^2 + X + 7 = (-X + 4) \cdot (-X^2 + 2X - 4) + (2X + 10) \\ a_2 = q_2 a_3 + a_4 & -X^2 + 2X - 4 = (6X + 10) \cdot (2X + 10) + 0 \end{array}$$

So this time we have a gcd of $2X + 10$ (or, if you please, $2X - 3$, which is the same in $\mathbb{Z}_{13}[X]$). Or, if you want a monic polynomial (i.e., leading coefficient 1), a gcd is $X + 5$.

Now to express our gcd as a linear combination, we write:

$$a_3 = a_1 - q_1 a_2 = a_1 - q_1(a_0 - q_0 a_1) = (1 + q_0 q_1)a_1 - q_1 a_0$$

where

$$1 + q_0 q_1 = 1 + 1(-X + 4) = -X + 5$$

So we have

$$(2X + 10) = (X - 4)(X^3 - 7X^2 + 3X + 3) + (-X + 5)(X^3 - 6X^2 + X + 7)$$

Hwk 58:

> In the ring $\mathbb{Z}[X]$, show that the ideal $(2, X) := \{2p + qX \mid p, q \in \mathbb{Z}[X]\}$ is *not* principal, i.e., it is *not* of the form $(g) := \{gp \mid p \in \mathbb{Z}[X]\}$. Show that the polynomials 2 and X do have a gcd, but that this gcd cannot be obtained as a linear combination of 2 and X.

Solution: We will show that a gcd is 1, and that it cannot be written as a linear combination of 2 and X. From these facts it will follow that the ideal $(2, X)$ is not principal.

(1) A divisor d of a polynomial p is a polynomial d such that another polynomial q exists with $dq = p$. By the degree formula ($\mathbb{Z}$ has no zero divisors, $\deg d + \deg q = \deg p$. So $\deg d \leq \deg p$. Any divisor of the constant polynomial 2 must therefore be a constant polynomial. And the constant in question must be a divisor of the integer 2. The divisors of 2 are therefore ± 2 and ± 1.

2 does not divide X, because from the equation $2q = X$ (an equation in $\mathbb{Z}[X]$, that can be interpreted as an equation in $\mathbb{Q}[X]$), it follows $q = \frac{1}{2}X \in \mathbb{Q}[X]$, but this polynomial is not in $\mathbb{Z}[X]$.

So $\gcd(2, X) = 1$ (or -1, which differs from 1 by a factor that is a unit in the ring.)

(2) Next we bring the assumption $1 = 2p + Xq$ for polynomials $p, q \in \mathbb{Z}[X]$ ($p = p_0 + p_1 X + \ldots p_k X^k$ and similar for q) to a contradiction. We look at the constant coefficient of the polynomials on either side and obtain $1 = 2p_0$. But such a $p_0 \in \mathbb{Z}$ doesn't exist.

(3) The proof that the ideal $(2, X)$ is not principal follows from the preceding two facts, and it is literally taken from the proof than in a PID, a gcd exists and can be written as a linear combination: Namely, assume that $(2, X) = (g)$. Then since $2 \in (2, X) = (g)$, 2 must be a multiple of g. Similarly, X must be a multiple of g. So g is a common divisor of 2 and X. Since $g \in (g) = (2, X)$, g must be a linear combination of 2 and X. Any common divisor of 2 and X must divide this linear combination, so it must divide g. This makes g a gcd of 2 and X. But these facts ar in contradiction to the previously shown facts that any gcd of 2 and X cannot be written as a linear combination.

Hwk 59:

> In the ring $\mathbb{Z}[\sqrt{-5}]$, show that the ideal $(1+\sqrt{-5}, 3) := \{(1+\sqrt{-5})a+3b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}$ is *not* principal, i.e., it is *not* of the form $(g) := \{gp \mid p \in \mathbb{Z}[\sqrt{-5}]\}$. Show that the numbers $1 + \sqrt{-5}$ and 3 do have a gcd, but that this gcd cannot be obtained as a linear combination of $1 + \sqrt{-5}$ and 3.

Solution: The proof logic proceeds along the same lines as before. – Note that $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$, and remember that $a + b\sqrt{-5} = c + d\sqrt{-5}$ implies $a = c, b = d$ by comparing real and imaginary parts.

(1) We have seen in a previous hwk that the only divisors of 3 in $\mathbb{Z}[\sqrt{-5}]$ are ± 1 and± 3. Now 3 does not divide $1 + \sqrt{-5}$, because the equation $3x = 1 + \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ could be interpreted as an equation in $\mathbb{C}$, where it has the (only) solution $x = \frac{1}{3} + \frac{1}{3}\sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}]$. The associate -3 doesn't divide $1 + \sqrt{-5}$ either. So the only choices for a gcd of 3 and $1 + \sqrt{-5}$ are the units ± 1.

(2) We bring the assumptions $1 = 3a + (1 + \sqrt{-5})b$ with $a, b \in \mathbb{Z}[\sqrt{-5}]$ to a contradiction. Let $a = a_1 + a_2\sqrt{-5}$ and $b = b_1 + b_2\sqrt{-5}$. Comparing real and imaginary part, we obtain $1 = 3a_1 + 1b_1 - 5b_2$ and $0 = 3a_2 + b_1 + b_2$. These are equations in $\mathbb{Z}$, and we can show that they have no solution by

reducing modulo 3: The first equation implies $1 \equiv b_1 + b_2$, whereas the second equation implies $0 \equiv b_1 + b_2$.

(3) By the very same argument as in the previous problem, the facts proved in (1),(2) cannot coexist with the hypothesis that the ideal $(3, 1+\sqrt{-5})$ is principal.

Hwk 60:

> In the ring $2\mathbb{Z}$ of even integers (which lacks a 1), show that the numbers 4 and 6 do not have a common divisor. *The definitions in class concerning principal ideals are not meant to carry over to rings without a 1, but would need to be modified. So no questions pertaining to ideals are asked for this example.*

Solution: The only divisor of 4 *in the ring* $2\mathbb{Z}$ is 2.
6 does not have any divisors *in the ring* $2\mathbb{Z}$, because 6 cannot be written as a product of even integers. In particular, there are no common divisors with 4.

Hwk 61:

> Give an example of a polynomial in $\mathbb{Q}[X]$ that is not prime (i.e. can be factored), but has no root in $\mathbb{Q}$. What is the smallest degree such a polynomial can have (explain why)?

Solution: If the polynomial has no rational root, then it has no linear factor. Since the polynomial can be factored, it must at least have degree 4. For instance, we could take $X^4-4 = (X^2-2)(X^2+2)$.

Hwk 62:

> Show that the polynomial $p = X^4 + 1$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{R}[X]$ nor in $\mathbb{C}[X]$. Give a complete factorization in $\mathbb{R}[X]$ (two quadratic factors; show that this is a complete factorization), and a complete factorization in $\mathbb{C}[X]$ by further factoring the real quadratics.
>
> Also give three different incomplete factorizations (product of two quadratics) in $\mathbb{C}[X]$ (for later use) by grouping the linear terms in two pairs in 3 different ways.

Solution: Since $X^4 + 1$ has no rational (nor real) root, any factorization within either $\mathbb{Q}[X]$ or $\mathbb{R}[X]$ can only be into two quadratics.

There are at least three ways now to show irreducibility in $\mathbb{Q}[X]$:

(1) If p factors in $\mathbb{Q}[X]$, then it factors in $\mathbb{Z}[X]$ as well, due to Gauss' lemma. So we can only have $p = (X^2 + aX + b)(X^2 + cX + d)$ with b, d *integers* satisfying $bd = 1$ and a, c integers. Checking the X^3 coefficient we must have $c = -a$. But $(X^2 + aX + 1)(X^2 - aX + 1) = X^4 + (2 - a^2)X^2 + 1$ and $(X^2 + aX - 1)(X^2 - aX - 1) = X^4 + (-2 - a^2)X^2 + 1$. And neither $2 - a^2$ nor $-2 - a^2$ will be zero for any integer a.

(2) If p factors in $\mathbb{Q}[X]$ then it trivially factors in $\mathbb{R}[X]$ (with the same factorization), since $\mathbb{Q} \subset \mathbb{R}$. So we find the only factorization in $\mathbb{R}[X]$ (see below): it is $X^4+1 = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$. Since this is not a factorization in $\mathbb{Q}[X]$, p is irreducible in $\mathbb{Q}[X]$.

(3) This is tricky, and you need both experience and an easy lemma (that wasn't covered in class) to find it: Namely, the substitution $X = Y + 1$ is a ring isomorphism between $\mathbb{Q}[Y]$ and $\mathbb{Q}[X]$; therefore $p(X)$ is irreducible if and only if $\tilde{p}(Y) = p(Y+1) = (Y+1)^4+1 = Y^4+4Y^3+6Y^2+4Y+2$ is irreducible. This latter polynomial is irreducible by Eisenstein's test with the prime number 2:

The leading coefficient is not divisible by 2, all other coefficients are, and the constant coefficient is not divisible by 2^2.

Now we show that X^4+1 can be factored in $\mathbb{R}[X]$. Proof: $X^4+1=(X^2+\sqrt{2}+1)(X^2-\sqrt{2}+1)$, as can be checked by expanding.

How would you *find* this factorization? You try to factor X^4+1 into quadratics. There is no loss of generality to have monic factors (monic= leading coefficient 1). So we try to find $a,b,c,d\in\mathbb{R}$ such that $X^4+1=(X^2+aX+b)(X^2+cX+d)$. Comparing coefficients, we get

$$a+c=0\ ,\quad b+d+ac=0\ ,\quad ad+bc=0\ ,\quad bd=1$$

Clearly $c=-a$, and the other conditions become

$$b+d=a^2\ ,\quad (d-b)a=0\ ,\quad bd=1$$

Clearly, $a\neq 0$, because else we would have $d=-b$, in contradiction to $bd=1$. So we conclude $b=d$ from the 2nd equation. $b=d$ must be positive from the first equation. So $b=d=1$ from the 3rd equation. Now we have $a=\pm\sqrt{2}$ from the 1st equation.

Solving the two quadratics in $\mathbb{C}$ gives us a complete factorization of p in $\mathbb{C}[X]$:

$$X^4+1=\Big(X-\frac{(1+i)\sqrt{2}}{2}\Big)\Big(X-\frac{(1-i)\sqrt{2}}{2}\Big)\Big(X-\frac{(-1+i)\sqrt{2}}{2}\Big)\Big(X-\frac{(-1-i)\sqrt{2}}{2}\Big)$$

Pairing the 1st with the 2nd, 3rd, 4th factor respectively, we get the following incomplete factorizations in $\mathbb{C}[X]$:

$$X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)=(X^2-\sqrt{2}iX-1)(X^2+\sqrt{2}iX-1)=(X^2+i)(X^2-i)$$

Hwk 63:

> In the fields $\mathbb{Z}_p$ for $p=2,3,5,7,11,13,17,19,23,29$, find one solution of the equations $x^2+1=0$, $x^2-2=0$, $x^2+2=0$ each, or conclude that none exists. Basically that's trial and error, and I have filled in all but three of the "doesn't exist" cases, and a few of the existence cases, to save you work. [Table with filled-in cases not recopied here.] Note also that in the example $p=29$, to find solutions, I only needed to test $1,2,3,\ldots,14$, since $15\equiv -14$, $16\equiv -13$,....
>
> Once this is accomplished, use the information, and wisdom gleaned from the very last part of the previous problem, to factor X^4+1 completely in $\mathbb{Z}_p[X]$ for the prime numbers $p=2,3,5,7,11,13,17$ (and more of them, if you are bored, or want to get bored).
>
> *Background info: a simple result from the theory of quadratic residues (in elementary number theory), or in other terms, a simple argument about groups, which we have alas no time to go into, implies in particular: if p is an odd prime such that there is no element in $\mathbb{Z}_p$ whose square is -1, and also no element whose square is 2, then there does exist an element whose square is -2.*
>
> *Accepting this fact, you can conclude that at least one of the factorizations of X^4+1 into quadratics (in $\mathbb{C}[X]$) found in problem 62 can serve as a model for factorization in $\mathbb{Z}_p[X]$; in other words: X^4+1 can be factored nontrivially in *every* $\mathbb{Z}_p[X]$.*

Solution: The table gives one solution x to the given equations in the rings (fields, actually) $\mathbb{Z}_p$. The negative of a solution is also a solution for these equations here. It turns out there are no

further solutions (because quadratic polynomials have only two roots, when the coefficient ring is a field), but this is not used in the following.

p	$x^2+1=0$	$x^2-2=0$	$x^2+2=0$
2	1	0	0
3	DNE	DNE	1
5	2	DNE	DNE
7	DNE	3	DNE
11	DNE	DNE	3
13	5	DNE	DNE
17	4	6	7
19	DNE	DNE	6
23	DNE	5	DNE
29	12	DNE	DNE

All coefficients will be congruence classes, even though they are written like integers, without a bar. Now we can copycat factorizations from $\mathbb{C}$: If in our finite field we have an a such that $a^2+1=0$, then we can factorize $X^4+1=(X^2+a)(X^2-a)$. If we have a b such that $b^2=2$, then we can factorize $X^4+1=(X^2-bX+1)(X^2+bX+1)$. If we have a c such that $c^2=-2$, then we can factorize $X^4+1=(X^2+cX-1)(X^2-cX-1)$. If we have all three of them, then we have a factorization into linear factors, which we could get, by taking the gcd of quadratics from two different factorizations.

Factorization in $\mathbb{Z}_2[X]$: $X^4+1=(X^2+1)(X^2-1)=(X^2+1)(X^2+1)=(X+1)^4$
Factorization in $\mathbb{Z}_3[X]$: $X^4+1=(X^2+X-1)(X^2-X-1)=(X^2+X+2)(X^2+2X+2)$
Factorization in $\mathbb{Z}_5[X]$: $X^4+1=(X^2-2)(X^2+2)=(X^2+2)(X^2+3)$
Factorization in $\mathbb{Z}_7[X]$: $X^4+1=(X^2-3X+1)(X^2+3X+1)=(X^2+3X+1)(X^2+4X+1)$
Factorization in $\mathbb{Z}_{11}[X]$: $X^4+1=(X^2+3X-1)(X^2-3X-1)=(X^2+3X+10)(X^2+8X+10)$
Factorization in $\mathbb{Z}_{13}[X]$: $X^4+1=(X^2-5)(X^2+5)=(X^2+5)(X^2+8)$
Factorization in $\mathbb{Z}_{17}[X]$ below.
Factorization in $\mathbb{Z}_{19}[X]$: $X^4+1=(X^2+6X-1)(X^2-6X-1)=(X^2+6X+18)(X^2+13X+18)$
Factorization in $\mathbb{Z}_{23}[X]$: $X^4+1=(X^2-5X+1)(X^2+5X+1)=(X^2+5X+1)(X^2+18X+1)$
Factorization in $\mathbb{Z}_{29}[X]$: $X^4+1=(X^2-12)(X^2+12)=(X^2+12)(X^2+17)$

Factorization in $\mathbb{Z}_{17}[X]$: three essentially different factorizations in quadratics (neither of them complete: the complete factorization is into 4 linear terms)

$$\begin{aligned} X^4+1 &= (X^2-4)(X^2+4)=(X^2+4)(X^2+13) \\ &= (X^2-6X+1)(X^2+6X+1)=(X^2+6X+1)(X^2+11X+1) \\ &= (X^2-7X-1)(X^2+7X-1)=(X^2+7X+16)(X^2+10X+16) \end{aligned}$$

We can obtain a complete factorization by calculating, e.g., the gcd of X^2+13 and X^2+6X+1, or by looking for roots for the individual quadratics. Either way, we find $X^4+1=(X-2)(X+2)(X-9)(X+9)=(X+2)(X+8)(X+9)(X+15)$

In connection with the Eisenstein irreducibility test, we have seen: If a monic polynomial in $\mathbb{Z}[X]$ is reducible in $\mathbb{Q}[X]$ (or equivalently in $\mathbb{Z}[X]$), then it is also reducible in every $\mathbb{Z}_p[X]$.

The problem we have just solved shows (provided we accept that no prime will have a triple DNE *entry in the above table), that the converse is not true. We have exhibited a polynomial that is reducible in every $\mathbb{Z}_p[X]$, but nevertheless irreducible in $\mathbb{Q}[X]$.*

Epilog: This is not part of the problem, but let me explain fyi why it is true for every odd prime number p, that among the equations $x^2+1=0$, $x^2-2=0$, $x^2+2=0$, either exactly one or all three have a solution in $\mathbb{Z}_p$:

Choose any $a\neq 0$ in $\mathbb{Z}_p$. If an equation $x^2=a$ has a solution x_1 in $\mathbb{Z}_p$, then $x_2:=-x_1$ is also a solution; and it is a different one, because p is odd. ($x=-x$ implies $x=0$ in $\mathbb{Z}_p$ with p odd). There

can be no further solution because the quadratic polynomial $x^2 - a$ can have only two roots. So if we take the squares of all elements $x \in \mathbb{Z}_p \setminus \{0\} =: \mathbb{Z}_p^*$, each result a that is obtained among these squares is obtained exactly twice. Which means that one half of the $p-1$ many elements of $\mathbb{Z}_p^*$ are squares and the other half are non-squares.

(1) Obviously the product of two squares is a square: $(x^2)(y^2) = (xy)^2$. — (2) It is easy to see that the product of a square and a non-square is a non-square. For if $x^2 b = y^2$, then $b = (yx^{-1})^2$, so b would have to be a square, too. This argument uses the fact that all elements of $\mathbb{Z}_p^*$ have a multiplicative inverse in the field $\mathbb{Z}_p$. — (3) Finally we can conclude that the product of two non-squares must be a square (and this will turn out ot be the crucial observation): Namely let $b \neq 0$ be a nonsquare. The mapping $x \mapsto bx\,,\ \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ is one-to-one and onto because its inverse is $y \mapsto b^{-1}y$. Since it maps the squares (of which there are $(p-1)/2$ many) into non-squares (which are equally many) according to part (2), there is no choice left for the non-squares but to be mapped into squares. But that means non-square times non-square is square.

Now since $(-1) \cdot 2 = (-2)$, not all three of these elements can be non-square. If -1 and 2 are both non-square, then -2 is square. If exactly one of -1 and 2 is non-square, then -2 is also non-square. If both -1 and 2 are square, then so is -2.

Hwk 64:

> We have seen that a polynomial of degree n in $F[X]$ can have at most n roots in F (or any extension field of F). This assumed that F be a field. In contrast, consider the polynomial ring $\mathbb{Z}_{25}[X]$.
>
> How many roots does the polynomial X^2 have in $\mathbb{Z}_{25}$?
>
> Give several essentially different factorizations of X^2 in $\mathbb{Z}_{25}$, thus showing that the unique factorization property may fail in $R[X]$, if R is not a field (and not even an integral domain).

Solution: The roots of X^2 in $\mathbb{Z}_{25}[X]$ are: 0, 5, 10, 15, 20. We have essentially distinct factorizations $X^2 = X \cdot X = (X+5)(X+20) = (X+10)(X+15)$.

We could even have further factorizations like $X^2 = (X - 5X^2)(X + 5X^2)$. However, note that $X + 5X^2 = X(1+5X)$, and $1+5X$ is a unit because $(1+5X)(1-5X) = 1$. So this factorization is not essentially different from the factorization $X \cdot X$.

Hwk 65:

> In $\mathbb{Z}_2[X]$, consider the ideal I of all multiples of the irreducible polynomial $X^3 + X + 1$. Denoting the equivalence class $\bar{X}_I$ in $\mathbb{Z}_2[X]/I$ as j, list all elements of $\mathbb{Z}_2[X]/I$, and give their multiplication table. In particular, find the inverse of $1 + j$ in the field $\mathbb{Z}_2[X]/I$.

Solution: Every congruence class modulo I contains exactly one polynomial of degree ≤ 2 (or the 0 polynomial). Since the coefficients can be only 0 or 1 in $\mathbb{Z}_2$, we can enumerate 8 congruence classes: $\overline{0}$, $\overline{1}$, $\overline{X}$, $\overline{1+X}$, $\overline{X^2}$, $\overline{1+X^2}$, $\overline{X+X^2}$, $\overline{1+X+X^2}$.

Let $j := \overline{X}$. Then we get the following multiplication table (from which the trivial cases 0 and 1 have been omitted):

$\cdot$	j	$j+1$	j^2	j^2+1	j^2+j	j^2+j+1
j	j^2	j^2+j	$j+1$	1	j^2+j+1	j^2+1
$j+1$	j^2+j	j^2+1	j^2+j+1	j^2	1	j
j^2	$j+1$	j^2+j+1	j^2+j	j	j^2+1	1
j^2+1	1	j^2	j	j^2+j+1	$j+1$	j^2+j
j^2+j	j^2+j+1	1	j^2+1	$j+1$	j	j^2
j^2+j+1	j^2+1	j	1	j^2+j	j^2	$j+1$

We just give one sample calculation proving this table: $(j^2+1)(j^2+j+1) = j^4+j^3+2j^2+j+1 = (j+1)(j^3+j+1)+j^2-j = j^2+j$.

From the table, we can in particular see that $(j+1)^{-1} = j^2+j$.