Algorithms HW

1. Let a and b be positive integers. Under what conditions do we have $(a) \supseteq (b)$? (This tells us what containment of ideals corresponds to in terms of integers.)

Although we are working with integers, note that in any ring R with $1 \neq 0$ we have $a = \sum_{i=1}^{a} 1 \in R$ and $b = \sum_{i=1}^{b} 1 \in R$ and so the following statements hold for any ring with $1 \neq 0$.

We have $(b) \subseteq (a)$ if and only if $b \in (a)$ or $b = c \cdot a$ for some $c \in R$. Now, since both a, b are positive multiples of 1 we have that $c \in \mathbb{Z}_{+}$. In other words, a divides b. This tells us that containment of such ideals is "relation reversing" compared with divisibility of integers. ∎

2. Consider the following true statements about positive integers. For each statement, write down the corresponding statement about ideals in a general ring, and determine whether it is true.

   - If a and b are coprime and if c divides b, then a and c are also coprime.
   - If a divides both b and c, then a divides $\gcd(b, c)$.
   - If a and b are coprime, then $\operatorname{lcm}(a, b) = ab$.
   - For any a and b, we have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

- a, b coprime means $gcd(a, b) = 1$. For the principal ideal domain $R = \mathbb{Z}$ we have that $(a, b) = (gcd(a, b))$. And so the corresponding statement for a general ring is: if $(a, b) = (1) = R$ and if $(b) \subseteq (c)$ then $(a, c) = (1)$. Note that a ring does not necessarily have a well-defined notion of a greatest common divisor of two elements, but it does if the ring also happens to be a UFD. Nevertheless, let us work with the statement above.

  This statement is true. The condition $(a, b) = (1)$ means that there exists elements $r_1, r_2 \in R$ such that $r_1 a + r_2 b = 1$, by definition of ideal generated by a set. Moreover, $(b) \subseteq (c)$ means there exists some $r_3 \in R$ such that $b = r_3 c$. Combining these statements we have

  $$1 = r_1 a + r_2 b = r_1 a + r_2 r_3 c \in (a, c).$$

  In other words, indeed, $(a, c) = 1$.

- Recall the discussion in question 1. The corresponding general statement is: if $(b) \subseteq (a)$ and if $(c) \subseteq (a)$ then $(b, c) \subseteq (a)$.

  This statement is again true. The hypothesis gives that there are elements $r_1, r_2 \in R$ such that $b = r_1 a$ and $c = r_2 a$. By definition, a general element of (b, c) is of the form $x_1 b + x_2 c$ for $x_1, x_2 \in R$. We have

  $$x_1 b + x_2 c = x_1 r_1 a + x_2 r_2 a = (x_1 r_1 + x_2 r_2) a \in (a).$$

  Hence, indeed, we have $(b, c) \subseteq (a)$.

- The corresponding general statement is: "if $(a, b) = (1)$ then $(a) \cap (b) = (ab)$". This statement is again true.

The hypothesis means that there are elements $r_1, r_2 \in R$ such that $r_1 a + r_2 b = 1$. We show that $(a) \cap (b) = (ab)$. The reverse inclusion is generally true since $ab = a \cdot b = b \cdot a$ and so $ab \in (a) \cap (b)$, becuase our rings are commutative.

Now we show the forward inclusion $(a) \cap (b) \subseteq (ab)$. Let $ca \in (a) \cap (b)$. By definition, there exists some $d \in R$ such that $db = ca$. Consider the following

$$\begin{aligned} ca - db &= 0 \\ r_2 ca - d(r_2)b &= 0 \\ r_2 ca - d(1 - r_1 a) &= 0 && \text{By our hypothesis} \\ (r_2 c + dr_1)a &= d \\ (r_2 c + dr_1)ab &= db \\ (r_2 c + dr_1)ab &= ra, \end{aligned}$$

That is we have found $ra = Kab$ for some $K \in R$ and so $ra \in (ab)$. Hence we have $(a) \cap (b) \subseteq (ab)$ and moreso $(a) \cap (b) = (ab)$.

■

3. Let R be a finite ring. Prove that R is a field if and only if it is an integral domain.

In general we have that R a field implies R is an integral domain, even if R is not finite. We recount the proof here. Suppose R is a field, that is R is commutative with $1 \neq 0$ and every $a \in R$ is a two-sided unit. Now suppose we have $ab = 0$. If $a = 0$ then we are done, so suppose a is non-zero in R. Then, a has a two-sided inverse $a^{-1} \in R$, and so

$$0 = ab = a^{-1}ab = 1 \cdot b = b.$$

If we instead assume $b \neq 0$ then an extremely similar calculation will show that $ab = 0$ implies $a = 0$. (Or, perhaps it's enough that R is commutative at this point?) Thus, R is an integral domain.

Now suppose R is finite and is an integral domain. That is, R is a commutative ring with $1 \neq 0$ and for all $a, b \in R$ we have $ab = 0$ implies $a = 0$ or $b = 0$. We show that every non-zero element in R has a two-sided inverse. Let $a \in R$ be some non-zero element and let $\phi_a : R \to R$ be the map defined by $\phi(r) = a \cdot r$.

We claim that ϕ_a is injective. Suppose we have $\phi(b) = \phi(c)$ for some $b, c \in R$. That is, $ab = ac$, equivalently $a(b - c) = 0$. But recall that a is a non-zero element in the integral domain R, and so we must have $b - c = 0$. In other words $b = c$ and ϕ_a is injective by definition.

In addition, since R is finite and $\#R = \#R$, we have that ϕ_a is actually a bijection. And so there must exist some $c \in R$ such that $\phi(c) = 1$. That is, we have $c \in R$ such that $ac = 1$. Since R is commutative, a is actually a two-sided unit with inverse c. Thus, R is a field.

Note to self: Aluffi claims that finite division rings turn out to always be commutative. Have a read of this later if we get time ■

4. Let $\mathbb{F}$ be a finite field of order q. We are going to prove that the multiplicative group $\mathbb{F}^\times$ is cyclic of order $q-1$.

   (a) Show that for all $d \geq 1$, the number of d-torsion elements of the group $\mathbb{F}^\times$ is at most d.

   (b) Suppose that G is a finite abelian group such that the number of d-torsion elements of G is at most d for all $d \geq 1$. Prove that G is cyclic. (Hint: the structure theorem for finite abelian groups may be helpful.)

(a) Consider the polynomial $f(x) = x^n - 1 \in \mathbb{F}[x]$. Recall that $\mathbb{F}[x]$ is a unique factorization domain we should probably understand this better, and so f has at most n roots in $\mathbb{F}$. That is, there are at most n elements in $\mathbb{F}$ such that $a^n = 1$. And, in particular, the zero element in the ring $\mathbb{F}$ does not satisfy the above equation. And so, all roots of f must in fact lie in $\mathbb{F}^\times$. Then, recalling that an element in a group $g \in G$ is a d-torsion element of G if $|g| \mid d$, the above shows that $\mathbb{F}^\times$ has at most d elements with d-torsion, for each $d \geq 1$. question: does d-torsion mean that $|g| = d$ or that $|g| \, |d$?

(b) I'm not sure we've super talked about the structure theorem of finite abelian groups much, so I will recall the theorem in detail here. *Theorem:* If G is a finite abelian group then we have that G is a product of cyclic groups, in particular

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z},$$

for $d_i > 0$ integers and where $d_1 \mid d_2 | \cdots | d_n$ ew, i hate the spacing on this. Moreover, $|G| = d_1 \cdots d_s$. Here, we are treating G as a group under addition.

Now suppose G is a finite abelian group such that the number of d-torsion elements is at most d for all $d \geq 1$. We show that $s = 1$ and so G is cyclic. Suppose, for contradiction, that $s > 1$ and let $g \in G$. We have that $\langle g \rangle \leq G$ and so, by Lagrange's theorem, we have that $|g| \mid |G| = d_1 \cdots d_s$. And so $|g|$ divides one of d_i. If $\langle g \rangle$ divides d_i then, since in particular $d_i | d_s$, we also have $\langle g \rangle | d_s$. Indeed, we have $m_1 |g| = d_i$ and $m_2 d_i = d_s$ then $m_1 m_2 |g| = d_s$, i.e., $|g| \, |d_s$. That is g is a d_s-torsion element.

We have shown that all elements $g \in G$ have d_s-torsion. However, we have $|G| =$

$d_1 \cdots d_s > d_s$. And so we have found more than d_s elements of G which have d_s-torsion, a contradiction. That is, we must in fact have $s = 1$ and $G \cong \mathbb{Z}/d\mathbb{Z}$ for some $d \in \mathbb{N}$. In other words, G is a cyclic group.

■

5. Let R be a ring and $f \in R$ an element. Prove that the localisation of R at the set $S = \{1, f, f^2, \dots\}$ is isomorphic to $R[x]/(1 - xf)$.

Let us first define a map into $R[x]$: $\phi : S^{-1}R \to R[x]$ by $\varphi(1/f) = x$ and $\phi(a/1) = a$, and then we extend this definition so that the map distributes over products and addition in $S^{-1}R$. That is $\phi(a/f^k) = ax^k$ and $\phi(a/f^k + b/f^\ell) = \phi((af^\ell + b^k)/f^{k+\ell}) = (af^k + bf^\ell)x^{k+\ell}$. Is this sufficient reasoning to allow us to "extend the map".

First we check that this is a well defined map out of $S^{-1}R$. Suppose $a/f^k \equiv b/f^\ell$ and consider

$$\phi(a/f^k - b/f^\ell) = \phi(\frac{af^\ell - bf^k}{f^{\ell+k}}) = (af^\ell - bf^k)x^{\ell+k}.$$

Now, the condition $a/f^k \equiv b/f^\ell$ means that there exists some $c \in S$ such that $c(af^\ell - bf^k) = 0$, in particular $c = f^m$ for some integer $m \geq 0$. That is, we have $f^m(af^\ell - bf^k) = 0$. Applying ϕ to both sides of this expression gives $x^m(af^\ell - bf^k) = 0$ in $R[x]$. If we somehow knew that $\ell + k \geq m$ we'd be done, but it's not super clear to me how we can finish this reasoning. This might also perhaps be the wrong approach

Actually note that $\phi : S^{-1}R \to R[x]$ is not a well-defined map, consider the image of $(af^2)/f^3$

Next we check that ϕ is in fact a well-defined map into the quotient $R[x]/(1 - fx)$. Namely, we will check that $\phi^{-1}((1 - fx)) = \{0\}$. We have

$$\phi^{-1}(1 - fx) = \frac{1}{1} - \frac{f}{f} = 0 \in S^{-1}R.$$

And so, ϕ is a well-defined map into the quotient $R[x]/(1 - fx)$. From now, we will treat ϕ as a map $\phi : S^{-1} \to R[x]/(1 - fx)$. Something about this paragraph feels a bit fishy to me, do we think that I checked everythign that I needed to check?

Nex we will show that ϕ is a bijection. First we check injectivity. Notice that every element of $S^{-1}R$ can be reduced to the form a/f^k for some $a \in R$ and some natural k. Now suppose $\phi(a/f^k) = \phi(b/f^\ell)$, i.e. $ax^k = bx^\ell$. The only way for this to be true is if $k = \ell$ and only if $a = b$ a part of me wants to unpack this, I believe this is true because intuitively "the constants in $R[x]$ are independent of the variable x." is there a more precise way of saying this?. That is, $a/f^k = b/f^\ell$ and so ϕ is injective.

Next we show that ϕ is surjective. Suppose $a_0 + a_1x + \cdots a_nx^n \in R[x]/(1 - fx)$, since this is an element of the quotient suppose we have reduced away all existing factors of f in each coefficient a_i using the relation $1 = fx$ in the quotient. Then notice $a_0/1 + a_1/f + \cdots a_n/f^n$ maps to the given polynomial under ϕ.

In the end, we have found a bijective homomorphism from $S^{-1}R$ to $R[x]/(1 - fx)$, and so these rings are isomorphic. ∎

6. Let p be a prime number, and let $\Phi_p(x)$ be the polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1\,.$$

By considering the polynomial $\Phi_p(x+1)$, or otherwise, show that $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$.

Recall Eisenstein's Criterion maybe cite it here

First we consider $\Phi(x)$ as a polynomial in $\mathbb{Z}[x]$ and after that, why is it also irreducible in $\mathbb{Q}[x]$?

Next, notice that $\Phi(x) = \frac{x^p-1}{x-1}$ i wonder how we show this? i vaugely recall that it is a combinatorial fact. perhaps we just multiply both sides by $x-1$

It then follows that $\Phi(x+1) = \frac{(x+1)^p-1}{x}$. Now, using the binomial theorem, we have

$$(x+1)^p = x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{3}x^3 + \binom{p}{2}x^2 + \binom{p}{1}x + 1.$$

And so

$$\frac{(x+1)^p-1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}.$$

We claim that this form allows us to deduce that the Eisenstein criterion is fulfilled. First, we have $a_n = 1$ and so a_n is not in any prime ideal. Moreover, we have that $\binom{p}{1} = p \notin (p)^2 = (p^2)$ in $\mathbb{Z}[x]$. is this last sentence true?

Then lastly, we need to show that $\binom{p}{k} \in (p)$ for each $1 < k < p$. i'm not entirely sure how the proof in the book works for this.. ∎

7. (Introduction to Newton polygons) There is a far-reaching generalisation of the Eisenstein irreducibility criterion, called the theory of Newton polygons. Let R be a unique factorisation domain and $p \in R$ a prime element. The *p-adic valuation* $v_p(a)$ of an element $a \in R$ is defined to be the number of times that p appears in the prime factorisation of a (or $v_p(a) = \infty$ if $a = 0$). The (p-adic) *Newton polygon* of a non-zero polynomial

$$f(x) = \sum_{i=0}^{d} a_i x^i \in R[x]$$

is defined to be the lower convex hull of the set

$$\{(i, v_p(a_i)) \,:\, 0 \le i \le d\}$$

in $\mathbb{R}^2$. This lower convex hull is a finite union of line segments. The *slopes* of the Newton polygon are defined to be the slopes of these line segments, and the *multiplicity* of a slope is the length of the projection of the corresponding line segment to the x-axis. We also adopt the convention that $-\infty$ is a slope of the Newton polygon if $a_0 = 0$, and the multiplicity of $-\infty$ is the smallest i such that $a_i \neq 0$.

The main theorem of Newton polygons states that if s is a slope of $f(x)$ and $g(x)$ of multiplicity m and n, respectively, then s is also a slope of $f(x)g(x)$ with multiplicity $m + n$. (If s is not a slope of f or g, count it with multiplicity 0.)

- When $R = \mathbb{Z}$, compute the 3-adic Newton polygons of

$$f(x) = x^2 + 3x + 3 \quad \text{and} \quad g(x) = x^3 + 3x - 1\,.$$

  What are their slopes (with multiplicity)? Compute the slopes (with multiplicity) of the 3-adic Newton polygon of the product $f(x)g(x)$, and check that your answer accords with the main theorem of Newton polygons.
- Use the main theorem of Newton polygons to give another proof of the Eisenstein irreducibility criterion.
- Use the main theorem of Newton polygons to show that the polynomial

$$x^5 + 15x^3 + 50x^2 + 100$$

  is irreducible in $\mathbb{Z}[x]$.
- Is the polynomial $x^4 + 4$ irreducible in $\mathbb{Z}[x]$?

-
-
- We show that $h(x) = x^5 + 15x^3 + 50x^2 + 100$ is irreducible over $\mathbb{Z}[x]$. Consider the

slope data for the 5-adic newton polytope for h, we have $(-1/2, 5)$ insert newton polytope figure Now suppose $h = fg$ for non-constant $f, g \in \mathbb{Z}[x]$. Without loss of generality, we have two cases: either $def(f) = 1$ and $deg(g) = 4$ or $deg(f) = 2$ and $deg(g) = 3$.

First consider $deg(f) = 1$ and $deg(g) = 4$. Consider the 5-adic newton polytope for f. Since f is degree 1 we can only have integer slopes in the p-adic newton polytope for f, for any p. And so, by the main theorem for p-adic newton polytopes, it's impossible to choose coefficients for f which is consistent with the slope data for h.

Likewise, if we instead have $deg(f) = 2, deg(g) = 3$ then we have a similar parity issue for the slopes of the 5-adic newton polytope for g. We know that $a_n(f) = a_n(g) = 1$ and so in particular $\nu_5(a_n(g)) = 0$. Hence to have a slope of $-1/2$ we must have $\nu_5(a_1(g)) = 1$ and $\nu_5(a_1(g)) \geq 1$. However, from here it is impossible to choose coefficients for a_0 which gives us another slope of length $-1/2$. Intuitively, there is "not enough room" for all the slopes to be $-1/2$ in the 5-adic newton polytope for g.

Lastly, since h is monic there is no constant term which divides all the coefficients of h, f, g. And so we cannot decompose h into a product of a non-unit constant and a degree 5 polynomial.

All cases lead us to contradiction, and so it must be that one of f, g is a unit, and so h is irreducible.

- Let $h(x) = x^4 + 4$ and consider the 2-adic Newton Polytope of f. Insert Newton polytope figure Representing the slope-length data in the format (Slope, Length) we have the following slope-length data $(-1, 1), (0, 3)$.

  Now suppose we can write $h(x) = f(x)g(x)$ for polynomials $f, g \in \mathbb{Z}[x]$. If f, g are non-constant polynomials then we have two cases to consider $deg(f) = 1, deg(g) = 3$ or $deg(f) = 2, deg(g) = 2$, since h is a degree 4 polynomial. In either case notice that we must have the following constant terms $a_0(f) = a_0(g) = \pm 2$, since $a_0(h) = 4$. Likewise we must have leading terms $a_n(f) = a_n(g) = 1$. It follows that in either case we must have $\nu_2(a_0(f)) = \nu_2(a_0(g)) = 0$.

Now consider the case where $deg(f) = 1, deg(g) = 3$. We claim that there are only two possible 2-adic newton polytopes for f. Since the total length data for h only contains slopes $-1, 0$ it must be that $\nu_2(a_1(f))$ is either 0 or 1, otherwise we would have slope data for f which is incompatible with the slope data for h. Thus, in one case we have slope data $(0, 1)$ or $(-1, 1)$ for f. insert NP figure

Suppose that we have slope data $(-1, 1)$ for f. By the main theorem of Newton Polytopes, we must then have slope data $(0, 3)$ for g. However, since $\nu_2(a_0(g)) = 1$ we must then have $\nu_2(a_i(g)) = 1$ for each $i = 0, 1, 2, 3$. However, this contradicts the fact that $\nu_2(a_n(g)) = 0$ which we determined earlier. And so f cannot have slope data $(-1, 1)$.

Suppose instead that f has slope data $(0, 1)$. Since $\nu_2(a_0(f)) = 1$ we must then have $\nu_2(a_1(f)) = 1$ also. However, this again contradicts the fact that $a_n(f) = 1$ from earlier.

Thus there is no case where $deg(f) = 1, deg(g) = 3$. Suppose instead then that $deg(f) = deg(g) = 2$. Since we have $\nu_2(a_0(f)) = \nu_2(a_0(g)) = 1$ and $\nu_2(a_2(f)) = \nu_2(a_2(g)) = 0$ there are only two possible 2-adic newton polytopes for f, g. Insert said newton polytopes below Both newton polytopes have slope data $(-1, 1), (0, 1)$. By the main theorem of newton polytopes, the slope data for $f \cdot g$ is then $(-1, 2), (0, 2)$ but this contradicts the slope data for h, $(-1, 1), (0, 3)$.

It turns out we have yet a couple more cases. We could also have the constant terms of f, g to be ± 4 and ± 1. We consider again the case where $deg(f) = 1, deg(g) = 3$. Suppose without loss of generality that $a_0(f) = \pm 4$ and $a_0(g) = \pm 1$. The only possible 2-adic Newton polytope for f has slope data $(-2, 1)$. It follows then, by the main theorem for Newton Polytopes, that g must have slope data $(0, 3)$. In other words, every coefficient of g must be non-zero and odd. Let us then write $f = 4 + x$ and $g = 1 + ax + bx^2 + x^3$ where $a, b \in 2\mathbb{Z} + 1$. Considering the x coefficient of fg gives us that $4a + 1 = 0$, which has no integer solutions. If, on the other hand, we had $a_0(f) = -4$ and $a_0(g) = -1$ we would have the same 2-adic newton polytopes and the same slope data as above. The same computation would then instead give us the condition that $-4a - 1 = 0$ which again has no integer solutions.

Now, still considering $deg(f) = 1$ and $deg(g) = 3$ consider the case where $a_0(f) = \pm 1$ and $a_0(g) = \pm 4$. The only possible 2-adic newton polytope for f has slope data $(0, 1)$ insert image. And so, by the main theorem for p-adic newton polytopes, we must have that 2-adic newton polytope for g must have slope data $(-2, 1), (0, 2)$. For g we know that $\nu_2(a_0(g)) = 2$ and $\nu_2(a_3(g)) = 0$ we must then have $\nu_2(a_1(g)) = 0$ but the last point is free $\nu_2(a_2(g)) \geq 0$. Writing $f = 1 + x$ and $g = 4 + ax + bx^2 + x^3$, where $a \in 2\mathbb{Z}, b \in \mathbb{Z}$, and considering the coefficients of fg gives us the following system of equations

$$\begin{aligned} a + 4 &= 0 \\ b + a &= 0 \\ 1 + b &= 0. \end{aligned}$$

There are no consistent solutions to this system of equations. If we instead have the case where $a_0(f) = -1$ and $a_0(g) = -4$ a very similar computation will instead give us the following system of equations

$$\begin{aligned} -a - 4 &= 0 \\ -b + a &= 0 \\ b - 1 &= 0, \end{aligned}$$

where $a \in 2\mathbb{Z}$ and $b \in \mathbb{Z}$. This system, again, has no solutions. And so the case where $deg(f) = 1$ and $deg(g) = 3$ is not possible.

Now, still considering the case where our constant terms are $\pm 1, \pm 4$, suppose instead that $deg(f) = deg(g) = 2$. Since f, g are the same degree, suppose without loss of generality that $a_0(f) = \pm 1$. Since we know that $a_2(f) = 1$ the only possible 2-adic newton polytope for f has slope data $(0, 2)$ insert image Thus, by the main theorem for p-adic newton polytopes, we must have that the 2-adic newton polytope for g has slope data $(-2,1),(0,1)$, which means $a_1(g)$ is odd. Let us write $f = 1 + ax + x^2$ and $g = 4 + bx + x^2$ where $a \in \mathbb{Z}$ and $b \in 2\mathbb{Z}+1$. Considering the coefficients of fg gives us the following system of equations

$$\begin{aligned} &b + 4a = 0 \\ &1 + ab = 0 \implies a = \pm 1, b = \mp 1. \end{aligned}$$

This system has no consisten solutions. If we instead have $a_0(f) = -1$ and $a_0(g) = -4$, our 2-adic newton polytopes do not change, and a similar calculation will then give us the following system

$$\begin{aligned} &-b - 4a = 0 \\ &-1 + ab = 0 \implies a = \pm 1, b = \pm 1, \end{aligned}$$

which again has no solutions. Hence we also cannot have $deg(f) = deg(g) = 2$.

All possible cases for f, g lead us to contradiction. And so it must then be that h is irreducible in $\mathbb{Z}[x]$.

∎

4

■