Notes on Alex Barrios' AWS2021 Lectures on Modular Forms

Nicholas Todoroff

March 1, 2021

1

Exercises

Exercise 1: Product of square expressables is square expressable

If $m = a^2 + b^2$ and $n = c^2 + d^2$, then

$$\begin{aligned} mn &= (ab)^2 + (ad)^2 + (bc)^2 + (bd)^2 \\ &= (ac)^2 + 2abcd + (bd)^2 + (ad)^2 - 2abcd + (bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

Exercise 2: Recursion on unique m-partitions

Let $s(n, m)$ be the number of ways up to permutations to express the nonnegative integer n as a sum of m unique positive integers. Let $\{a_k\}_{k=1}^m$ be such a partition, i.e. $n = \sum_k a_k$. Then there are two cases: there is exactly one j such that $a_j = 1$, or $a_k \neq 1$ for all k. Write $n - m = \sum_k (a_k - 1)$. In the first case each term in the sum is nonzero except for the j^{th}, and the number of ways to write $n - m$ like this is $s(n - m, m - 1)$. In the second case, each term is nonzero for all k, so the number of ways to write $n - m$ like this is $s(n - m, m)$. So altogether $s(n, m) = s(n - m, m - 1) + s(n - m, m)$. Together with the conditions $s(n, n) = 1$ and $s(n, m) = 0$ if $n < m$, this gives a full recursive algorithm for computing $s(n, m)$. Below is some Julia code implementing this algorithm and calculating $s(50, 7) = 522$.

```
function s(n, m)
  if n < m
      0
  elseif m == 1
      1
  else
      s(n - m, m - 1) + s(n - m, m)
```

```
  end
end

s(50, 7)
```

Exercise 3: $\theta(q)^k$ counts ways to sum squares

Define

$$\theta(q) = \sum_{n\in\mathbb{Z}} q^{n^2}, \quad r_k(n) = \#\left\{(a_1,\dots,a_k)\in\mathbb{Z}^k \;\middle|\; \sum_{j=1}^k a_j^2 = n\right\}.$$

Then we wish to show that $\theta(q)^k = \sum_{n=0}^\infty r_k(n)q^n$. But it follows immediately by the definition of θ and r_k that

$$\theta(q)^k = \prod_{j=1}^k \sum_{a_j\in\mathbb{Z}} q^{a_j^2} = \sum_{(a_1,\dots,a_k)\in\mathbb{Z}^k} q^{a_1^2+\dots+a_k^2} = \sum_{n=0}^\infty r_k(n)q^n$$

since there is a term $q^{a_1^2+\dots+a_k^2}$ exactly when $n = \sum_{j=1}^\infty a_j^2$; by definition there are exactly $r_k(n)$ such terms.

Exercise 4: What numbers are sums of squares?

First, we prove Fermat's sum of two squares theorem.

Theorem. *Let p be an odd prime. Then $p = a^2 + b^2$ for integers a, b iff $p \equiv 1 \pmod 4$*

Proof. If $p = a^2+b^2$, then $p = (a+bi)(a-bi)$ and both a and b are nonzero (since otherwise p would be square). By Theorem A.1, if $p \equiv 3 \pmod 4$ then p is a Gaussian prime, and this factorization would not be possible. So $p \equiv 1 \pmod 4$.

If $p \equiv 1 \pmod 4$, then there is a Gaussian integer z such that $p = z\overline{z}$, so for $z = a+bi$ we have $p = a^2+b^2$. □

We now show that a positive integer $n > 2$ is a sum of two squares iff for any prime $q \equiv 3 \pmod 4$ the greatest k such that $q^k \mid n$ is even.

If $n = a^2+b^2$, then $n = (a+bi)(a-bi)$. A prime $q \equiv 3 \pmod 4$ is a Gaussian prime, so if $q \mid n$ then q must divide at least one of $a \pm bi$; but these are conjugates and q is real, so q must divide both and $q^2 \mid n$. A simple inductive argument on n/q^k shows that the largest k such that $q^k \mid n$ must be even.

Suppose now that for any prime $q \equiv 3 \pmod 4$, the greatest k such that $q^k \mid n$ is even. Any n can be written as $n = a^2 b$ where b is a product of distinct prime factors (potentially an empty product). We cannot have $q^k \mid b$ unless $k = 0$ since k is even and would imply that there is more than one factor of q in b; so every prime $p \mid b$ must have $p \equiv 1 \pmod 4$. But these can be written as the sum of two square by the above theorem, so b is a sum of two squares by recursive application of Exercise 1. Thus $n = a^2 b$ is a sum of two squares.

3

Stabilized Zeros

Let $f : \mathcal{H} \to \mathbb{C}$ be a modular form of weight k. When $k = 4$, consider that $\tau = e^{2\pi i/3}$ has $\tau = \frac{1}{\tau} - 1 = \frac{-\tau-1}{\tau} = \gamma\tau$, where $\gamma = (-1, -1; 1, 0) \in \mathrm{SL}_2(\mathbb{Z})$. Thus

$$f(\tau) = f\left(\frac{-\tau - 1}{\tau}\right) = \tau^4 f(\tau),$$

so since $\tau^4 = \tau \neq 1$ it must be that $f(\tau) = 0$. So τ must be a zero of *any* weight-4 form. It is interesting to consider this sort of situation in generality.

What's happening here is that γ is in the stabilizer of τ, and has $(j(\gamma, \tau))^k \neq 1$, where $j(\gamma, \tau) = c\tau + d$ when $\gamma = (a, b; c, d)$. Consider some $\tau \in \mathcal{H}$ stabilized by a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We must have

$$\begin{aligned} \tau = \gamma\tau = \frac{a\tau + b}{c\tau + d} &\implies c\tau^2 + (d - a)\tau - b = 0 \\ &\implies \begin{cases} b = 0 & \text{if } c = 0, \\ \tau = \frac{1}{2c}\left(a - d \pm \sqrt{(a-d)^2 + 4bc}\right) & \text{if } c \neq 0. \end{cases} \end{aligned}$$

We get $b = 0$ when $c = 0$ since $a = d = \pm 1$; in this case $\gamma = \pm 1$. (The -1 case tells us that the only odd-weight form is the zero function.) When $c \neq 0$, consider the discriminant:

$$\begin{aligned} (a - d)^2 + 4bc &= a^2 + d^2 - 2ad + 4bc \\ &= a^2 + d^2 + 2ad - 4(ad - bc) \\ &= (a + d)^2 - 4 \\ &= T^2 - 4, \end{aligned}$$

where $T = \mathrm{tr}(\gamma) = a + d$. Since $\tau \in \mathcal{H}$, we must have the $+$ branch and $T^2 - 4 < 0 \implies |T| < 2$. Since $j := j(\gamma, \tau) = c\tau + d$, we can write $\tau = \frac{j-d}{c}$ and thus

$$\begin{aligned} \frac{j - d}{c} = \tau = \frac{1}{2c}&\left(a - d + i\sqrt{4 - T^2}\right) \\ \implies 2j &= T + i\sqrt{4 - T^2} \qquad (3.1) \\ \implies j^2 &- jT + 1 = 0. \qquad (3.2) \end{aligned}$$

(3.2) is equivalent to the original stabilizer equation when $c \neq 0$, and is strikingly simple. When $T = 0$, we have $j = i$. For $T \neq 0$, (3.1) tells us that

$$|j|^2 = \frac{T^2}{4} + \frac{4 - T^2}{4} = 1, \qquad (3.3)$$

$$\arg(j) = \arctan\frac{\sqrt{4 - T^2}}{T} = \arctan\sqrt{4/T^2 - 1} = \arccos\frac{T}{2}.$$

Since $|T| = 0, \pm 1$ this means $j = \omega$ or $j = \omega^2$ where $\omega = e^{\pi i/3}$, the first primitive 6^{th} root of unity. Note that (3.3) is consistent with the fact that

$$\mathrm{Im}(\tau) = \mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|j|^2}.$$

Let $f : \mathcal{H} \to \mathbb{C}$ satisfy the modularity condition with weight k. This function has a zero at out stabilized τ when $j^k \neq 1$, meaning j is not a k^{th} root of unity. But

$$\begin{aligned} i \text{ is a } k^{\text{th}} \text{ root of unity} &\iff 4 \mid k, \\ \omega, \omega^2 \text{ is a } k^{\text{th}} \text{ root of unity} &\iff 6 \mid k. \end{aligned}$$

We don't care about the $3 \mid k$ case for ω^2 since we must have k even so that f is non-trivial. Altogether, we have the following result:

Proposition. *Let $f : \mathcal{H} \to \mathbb{C}$ such that $f \not\equiv 0$ satisfies the modularity condition with weight k, and suppose that there is $\tau \in \mathcal{H}$ and $\gamma = (a, b; c, d) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \neq \pm 1$ and $\gamma\tau = \tau$. Then $c \neq 0$, $\tau = \frac{j(\gamma,\tau) - d}{c}$, and exactly one of the following is true:*

(1) $\mathrm{tr}(\gamma) = 0$, $j(\gamma, \tau) = i$, *and* $f(\tau) = 0$ *if* $4 \nmid k$.

(2) $\mathrm{tr}(\gamma) = 1$, $j(\gamma, \tau) = \omega$, *and* $f(\tau) = 0$ *if* $6 \nmid k$.

(3) $\mathrm{tr}(\gamma) = -1$, $j(\gamma, \tau) = \omega^2$, *and* $f(\tau) = 0$ *if* $6 \nmid k$.

Conversely, if $\tau = \frac{j-d}{c}$ where $j = i, \omega, \omega^2$ and $c, d \in \mathbb{Z}$ and $c \neq 0$, then there is a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \neq \pm 1$ and $\gamma\tau = \tau$.

This result can likely be seen (perhaps more intuitively) by considering that points in the fundamental domain $\mathcal{F} = \left\{\tau \in \mathcal{H} \;\middle|\; |\mathrm{Re}(\tau)| \leq \frac{1}{2},\ |\tau| \geq 1\right\}$ which are nontrivially stabilized are exactly i, ω, ω^2, though I think the direct approach above is interesting.

To tie the Proposition into very first observation: $\tau = e^{2\pi i/3} = \omega^2$ is a zero of a weight-4 form because $6 \nmid 4$.

Umbral Calculus

The umbral calculus is the informal observation that we can treat a sequence $(B_k)_{k=0}^{\infty}$ as if an exponentiated variable, and perform formal manipulations as such. Formally, we can achieve this by noting that a (partial) function, for example $T : \mathbb{C}[[b]] \nrightarrow \mathbb{C}$, may be defined by $T(b^k) = B_k$ and extended linearly. This is necessarily a partial function since $T(\sum_k a_k b^k) = \sum_k a_k B_k$ must converge in order to make sense. For simplicity, we will say that $f(b) \equiv g(b)$ modulo T if $T[f(b)] = T[g(b)]$. First, some notes on formal power series.

Formal Power Series

A good reference is [1]. Let R be a ring. There are two way to define a topology on $R[[x]]$ which gives us $\sum_{k=0}^{\infty} a_k x^k$ as a convergent series and allows us to define $\sum_{k=0}^{\infty} \alpha_k$ for

$\alpha_k \in R[[x]]$. We will see that this notion of convergence is the same as the definition of *admissable sum* from [1].

We first consider the (x)-adic topology, where (x) is the ideal generated by x, i.e. the set of all power series with constant term equal to 0. A subset $U \subset R[[x]]$ is defined to be open in this topology if for every $\alpha \in U$ we have $\alpha + (x)^n R[[x]] \subset U$ for every positive integer n. It is evident that $\{\alpha + (x)^n R[[x]] \mid n \in \mathbb{Z}_+\}$ forms a neighborhood base for α. We proceed by calculating $\alpha + (x)^n R[[x]]$.

Lemma 3.1. *$(x)^n = R_n[[x]]$, the set of all power series of order n for n a positive integer.*

Proof. Evidently $(x)^n \subset R_n[[x]]$. If $\sum_{k=n}^{\infty} a_k x^k \in R_n[[x]]$, then

$$\sum_{k=n}^{\infty} a_k x^k = x^{n-1} \sum_{k=1}^{\infty} a_{k+n-1} x^k = xx\cdots x \sum_{k=1}^{\infty} a_{k+n-1} x^k,$$

which is an element of $(x)^n$, so $(x)^n = R_n[[x]]$. $\square$

Similarly, $(x)^n R[[x]] = R_n[[x]]$. So an element of $\alpha + (x)^n R[[x]] = \alpha + R_n[[x]]$ is of the form

$$\sum_{k=0}^{n-1} a_k x^k + \sum_{k=n}^{\infty} (a_k + b_k) x^k,$$

where $\alpha = \sum_{k=0}^{\infty} a_k x^k$ and $(b_k \in R)_{k=n}^{\infty}$ is arbitrary. A sequence $(\alpha_j)_{j=1}^{\infty}$ converges to α if for every open $U \ni \alpha$ there is a N such that $\alpha_n \in U$ for all $n \geq N$. Using the neighborhood base, this means that for every m there is an N such that $\alpha_n = \alpha + \sum_{k=m}^{\infty} b_k x^k$ for some (b_k). For a series $\alpha_j = \sum_{k=0}^{j-1} \beta_j$ with $\beta_j \in R[[x]]$ this criterion is exactly that of an admissable sum: α and (b_k) must be

$$\alpha = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{\infty} \beta_{jk} \right) x^k, \quad b_k = 0 \text{ for each } k,$$

where $\beta_j = \sum_{k=0}^{\infty} \beta_{jk} x^k$; the sum $\sum_{j=0}^{\infty} \beta_{jk}$ must be finite to make sense, so it must be that $\beta_{jk} = 0$ for large enough j. For $\alpha_j = \sum_{k=0}^{j-1} a_k x^k$ we obviously have convergence to any α.

Now we consider the $R[[x]]$ as the space of sequence $R^{\mathbb{N}}$, and give R the discrete topology and $R^{\mathbb{N}}$ the product topology. A base for this topology is given by

$$\left\{ \prod_{k=1}^{\infty} U_k \;\middle|\; U_k \subsetneq R \text{ for finitely many } k,\ U_k = R \text{ otherwise} \right\}.$$

In particular, $\prod_k U_k$ where

$$U_k = \begin{cases} \{a_k\} & \text{if } k \in J, \\ R & \text{otherwise} \end{cases}$$

is a neigborhood for any $\alpha = \sum_{k=0}^{\infty} a_k x^k$. So if $(\alpha_j)_{j=1}^{\infty}$ converges to α, then for every finite $J \subset \mathbb{N}$ there is an N such that for every $n \geq N$ we have $\alpha_{nj} = a_j$ for each $j \in J$ and $\alpha_n = \sum_{k=0}^{\infty} \alpha_{nk} x^k$. So for large enough n, we can make as many of the coordinates of α_n the same as those of α as we desire. This is evidently the same situation as with the (x)-adic topology.

Stuff

Definition 1. An *umbral operator for x_j* is a partial linear operator

$$T : R[[x_1, \dots, x_{j-1}, x_j, x_{j+1}, \dots, x_n]] \nrightarrow R[[x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n]]$$

such that

$$T(x_1^{k_1} \cdots x_{j-1}^{k_{j-1}} x_j^{k_j} x_{j+1}^{k_{j+1}} \cdots x_n^{k_n}) = A_{k_j} x_1^{k_1} \cdots x_{j-1}^{k_{j-1}} x_{j+1}^{k_{j+1}} \cdots x_n^{k_n}$$

for some sequence $(A_k \in R)_{k=0}^{\infty}$ and any nonnegative integers $k_1, \dots, k_n$.

Lemma 3.2. *Let $T : \mathbb{R}[[b, x]] \to \mathbb{R}[[x]]$ be an umbral operator for b. Then*

$$T \sum_{j,k=0}^{\infty} a_{jk} b^j x^k = \sum_{k=0}^{\infty} \left(T \sum_{j=0}^{\infty} a_{jk} b^j \right) x^k,$$
$$T(f(x)g(b,x)) = f(x)T(g(b,x)).$$

Exercises

<u>Exercise 1</u>: Recursive formula for Bernoulli numbers

Let $T : \mathbb{R}[[b]] \nrightarrow \mathbb{R}$ be the umbral operator for the Bernoulli number, i.e. $T[b^k] = B_k$ for all $k \in \mathbb{N}$. Then by definition of the Bernoulli numbers, modulo T we have

$$e^{bx} \equiv \frac{x}{e^x - 1},$$

where $x \in \mathbb{R}$ with $|x| < 2\pi$ and the right hand side is to be understood as an element of $\mathbb{R}$ (since it contains no explicit b). Thus

$$e^{bx}(e^x - 1) \equiv x \implies e^{(b+1)x} \equiv e^{bx} + x.$$

It follows from expanding into power series that that $(b+1)^m \equiv b^m$ if $m \neq 1$. So then

$$\sum_{k=0}^{m} \binom{m}{k} b^k \equiv b^m \implies \sum_{k=0}^{m-1} \binom{m}{k} b^k \equiv 0 \implies mb^{m-1} \equiv -\sum_{k=0}^{m-2} \binom{m}{k} b^k.$$

Reindexing and applying T, we finally get

$$(m+1)B_k = -\sum_{k=0}^{m-1} \binom{m+1}{k} B_k.$$

Appendix

Classification of Gaussian Primes

Contained herein is a classification of Gaussian primes together with the various facts of ring theory that I had to review in order to understand the proof; I do not provide proofs for all such facts. All rings are unital and commutative, though many results extend to noncommutative rings easily.

Theorem A.1 (Classification of Gaussian Primes)**.** *Let $p \in \mathbb{Z}[i]$ be prime. Then for one of $p, ip, -p, -ip$, exactly one of the following is true:*

(1) $p = 1 + i$.

(2) $\overline{p}$ *is a non-associated prime,* $|p|^2$ *is prime in* $\mathbb{Z}$*, and* $|p|^2 \equiv 1 \pmod 1$.

(3) p *is prime in* $\mathbb{Z}$ *and* $p \equiv 3 \pmod 4$.

Proof. The following proof is paraphrased from the one by "Zen Chonoles" at https://math.stackexchange.com/questions/172284/are-there-any-elegant-methods-to-classify-of-the-gaussian-primes. First, note that any associates of a prime (and only those) in $\mathbb{Z}[i]$ are also prime, since by Lemma A.3 they are the only other elements which generate the same ideal. For a prime p, these are exactly $ip, -p, -ip$.

We will let OPBC stand for "Order-Preserving Bijective Correspondence".

Instead of $\mathbb{Z}[i]$ directly we consider $R = \mathbb{Z}[x]/(x^2+1)\mathbb{Z}[x]$, wherein we use $(a)A$ to denote the principal ideal generated by a in the ring A. Consider $\mathbb{Z}$ as a subset of R and let $\iota : \mathbb{Z} \to R$ be the inclusion. Then by the Lattice Theorem, each prime R-ideal $Q \subset R$ has an associated prime $\mathbb{Z}$-ideal $(q)\mathbb{Z} = \iota^{-1}[Q]$ for some prime q, and $(q)\mathbb{Z} \subset Q$ since ι is the inclusion. But $(q)\mathbb{Z} \subset Q$ iff $q \in Q$ iff $(q)R \subset Q$. We then have

$$R/(q)R \cong \mathbb{F}_q[x]/(x^2+1)\mathbb{F}_q[x],$$

which is detailed in Lemma A.2. By the Correspondence and Lattice Theorems, the ideals of $R/(q)R$ are in OPBC with the ideals of R containing $(q)R$, and by the Lattice Theorem with the above isomorphisms they are also in OPBC with the ideals of $F_q := \mathbb{F}_q[x]/(x^2+1)\mathbb{F}_q[x]$. By Correspondence, these are in OPBC with the prime ideals of $\mathbb{F}_q[x]$ which contain x^2+1, and it is these that we classify.

If $q = 2$ then $x^2+1 = (x+1)^2$, and $(x+1)\mathbb{F}_2[x]$ is the only prime ideal containing this. This is prime by Lemma A.4, and by the same Lemma any prime must be irreducible, so this is the only one. Back in $R \cong \mathbb{Z}[i]$, this corresponds to $1+i$ (which is prime by Lemma A.5) since $(1+i)(1-i) = 2$.

If $q \equiv 1 (\text{mod} 4)$, then $x^2 = -1$ has a solution in $\mathbb{F}_q$ by Lemma A.7, so $x^2+1 = (x+a)(x-a)$ in $\mathbb{F}_q[x]$ for some $a \in \mathbb{F}_q$. Similar to above, there are thus exactly two prime ideals $(x+a)\mathbb{F}_q[x]$ and $(x-a)\mathbb{F}_q[x]$. In F_q, we have $(x+q)F_q \cdot (x-a)F_q = (0)F_q$; this must mean that these ideals correspond to primes $\pi_1, \pi_2 \in \mathbb{Z}[i]$ such that $(\pi_1)\mathbb{Z}[i] \cdot (\pi_2)\mathbb{Z}[i] = (q)\mathbb{Z}[i]$, which (for appropriate associates) gives $\pi_1\pi_2 = q$ and so $\overline{\pi}_1 = \pi_2$ since π_1, π_2 are prime.

If $q \equiv 3 \pmod 4$, then $x^2 = -1$ has no solution in $\mathbb{F}_q$ by Lemma A.7, so x^2+1 is irreducible. Thus F_q is a field by Proposition A.4 and has exactly one prime ideal, $(0)F_q$. This corresponds to $(q)\mathbb{Z}[i]$, so q itself is prime. □

Lemma A.2. *Let $R = \mathbb{Z}[x]/(x^2+1)$ and $q \in \mathbb{Z}$ be prime. We identify $\mathbb{Z}$ as a subset of R. Then $S := R/(q) \cong \mathbb{F}_q[x]/(x^2+1) =: T$.*

Proof. An element of S is an equivalence class $[f]_S = \{[f]_R + qG \mid G \in R\}$ for some $f \in \mathbb{Z}[x]$, and an element of T is an equivalence class $[\alpha]_T = \{\alpha + (x^2+1)\beta \mid \beta \in \mathbb{F}_q[x]\}$ for some $\alpha \in \mathbb{F}_q[x]$. Let $\pi : \mathbb{Z}[x] \to \mathbb{F}_q[x]$ be the projection which takes a polynomial in $\mathbb{Z}[x]$ to it's residue modulo q, and let $\iota : \mathbb{F}_q[x] \to \mathbb{Z}[x]$ be the map

$$\iota(0) = 0,\ \iota(1) = 1,\ \ldots,\ \iota(q-1) = q-1, \quad \iota\left(\sum_k a_k x^k\right) = \sum_k \iota(a_k) x^k.$$

Note that this is not a homomorphism, since e.g. if $q = 5$ then $\iota(4+4) = \iota(8) = \iota(3) = 3$ but $\iota(4) + \iota(4) = 4 + 4 = 8$.

Define $\phi : S \to T$ by $\phi([f]_S) = [\pi(f)]_\alpha$ for any $f \in \mathbb{Z}[x]$. This is well defined, since for any $h = f + (x^2+1)f'$ for some $f' \in \mathbb{Z}[x]$

$$\begin{aligned}
\phi([f]_S) = [\pi(f)]_T &= \left\{\pi(f) + (x^2+1)\beta \;\middle|\; \beta \in \mathbb{F}_q[x]\right\} \\
&= \left\{\pi(f) + (x^2+1)(\beta + \pi(f')) \;\middle|\; \beta \in \mathbb{F}_q[x]\right\} \\
&= \left\{\pi(f + (x^2+1)f') + (x^2+1)\beta \;\middle|\; \beta \in \mathbb{F}_q[x]\right\} \\
&= [\pi(h)]_T = \phi([h]_S).
\end{aligned}$$

This is automatically a homomorphism, since the equivalence classes must respect ring operations and π is a homomorphism. We can then define a map $\psi : T \to S$ by $\psi([\alpha]_T) = [\iota(\alpha)]_S$ and similarly show that it is well defined, and also a homomorphism. The key point is that if $\alpha = \beta + (x^2+1)\gamma$ for some $\alpha, \beta, \gamma \in \mathbb{F}_q[x]$, then

$$\iota(\alpha) = \iota(\beta) + \iota((x^2+1)\gamma) + q\delta$$

for some $\delta \in \mathbb{F}_q[x]$, which is so say that ι is a homomorphism modulo q.

The map ι is a right inverse for π, i.e. $(\pi \circ \iota)(\alpha) = \alpha$, and modulo q is also a left inverse, i.e. $[(\iota \circ \pi)(f)]_S = [f]_S$. It follows that $\psi = \phi^{-1}$, and so ϕ is an isomorphism. □

Proposition (Lattice Theorem). *Let $\phi : R \to S$ be a ring homomorphism and $I \subset J$ be ideals of S. Then $\phi^{-1}[I]$ is an ideal, and $\phi^{-1}[I] \subset \phi^{-1}[J]$. Furthermore, if I is prime then $\phi^{-1}[I]$ is also prime.*

Proposition (Correspondence Theorem). *Let $\phi : R \to S$ be a surjective ring homomorphism. Then there is a bijective correspondence between the ideals of S and the ideals of R containing* $\ker(\phi)$.

Lemma A.3. *Let R and $a, b \in R$. If there is a unit $u \in R$ such that $a = ub$, then $(a) = (b)$. If R is an integral domain, then the converse holds as well.*

Proof. Suppose $a = ub$. If $x \in (a)$, then $x = \alpha a$ for some $\alpha \in R$, and so $x = \alpha ub \in (b)$. So $(a) \subset (b)$. If $x \in (b)$, then $x = \beta b = \beta u^{-1} ub = \beta u^{-1} a$ for $\beta \in R$, and so $x \in (a)$. So $(a) = (b)$.

Suppose R is an integral domain and that $(a) = (b)$. Then there are $\alpha, \beta \in R$ such that $\alpha a = b$ and $a = \beta b$. It follows that $a = \beta\alpha a \implies 1 = \beta\alpha$, so α and in particular β are units. □

Proposition A.4. *Let R be a ring. Then*

(1) *$I \subset R$ is a maximal ideal iff R/M is a field.*

(2) *Every maximal ideal of R is prime.*

(3) *If R is a PID, then (r) is maximal for any irreducible $r \in r$ (and hence prime).*

(4) *If R is an integral domain, then every prime element is irreducible. (Hence, if R is a PID then every nontrivial prime ideal is maximal.)*

Proof. **(1)** If I is maximal, then consider the projection $\pi : R \to R/I$. By the Correspondence Theorem, the ideals of R/I correspond to those of R which contain I. But the only such ideals are M and R, so R/I has exactly two ideals and must be a field. Conversely, if R/I is a field, then $I = \pi^{-1}[(0)] \subset \pi^{-1}[R/I] = R$ by the Lattice Theorem, but these are the only ideals that contain I by Correspondence so any other ideal J with $I \subset J \subset R$ must have $J = I$ or $J = R$, so I is maximal.

(2) Let $M \subset R$ be a maximal ideal. Then R/M is a field with projection $\pi : R \to R/M$. The ideal $(0) \subset R/M$ is prime since a field cannot have zero divisors, so by the Lattice Theorem $\pi^{-1}[(0)] = M$ is prime.

(3) Suppose that there is an ideal I such that $(r) \subset I \subsetneq R$. Then since R is a PID, there is an $i \in I$ with $(i) = I \supset (r)$. So there is $x \in R$ such that $r = xi$, but r is irreducible so at least one of x, i are units. If i is a unit, then $(i) = (i^{-1}i) = (1) = R$ by Lemma A.3, which is impossible. If x is a unit, then $(r) = (xi) = (i)$ be the same Lemma.

(4) Suppose R is an integral domain and let $p \in R$ be prime such that $p = ab$ for some $a, b \in R$. Then $p|ab$, so $p|a$ or $p|b$. WLOG, assume its b. Then $b = \beta p$ for some $\beta \in R$, and $p = a\beta p \implies 1 = a\beta$, so a, β are units. So for any factorization of p, one factor must be a unit; thus p is irreducible. □

Lemma A.5. $1 + i \in \mathbb{Z}[i]$ *is prime.*

Proof. If $1 + i = (a + bi)(c + di)$, then $2 = |1 + i|^2 = (a^2 + b^2)(c^2 + d^2)$. But then the only possibilites are three of a, b, c, d are equal to 1 and the remaining equal to 0. This corresponds to $1 + i$ and its associates, so $i + 1$ is prime. □

Lemma A.6 (Wilson's Theorem)**.** *Let $q \in \mathbb{N}$ be prime. Then $(q - 1)! \equiv -1 \pmod{q}$.*

Proof. The full Wilson's Theorem includes the converse, but we do not need this result.

This is trivial if $q = 2$, so suppose q is odd. Since the integers modulo q form a field $\mathbb{F}_q$, every non-zero n has a multiplicative inverse modulo q. The only $a \in \mathbb{F}_q$ with $a = a^{-1}$ are $a = \pm 1$, and every other non-zero element of $\mathbb{F}_q$ has a distinct and unique inverse. Since $(q - 1)! = (q - 1)(q - 2) \cdots (2)(1)$, every element not ± 1 can be paired with it's inverse, leaving us with $(q - 1)! \equiv -1 \cdot 1 = -1 \pmod{q}$. □

Lemma A.7. *There is an $x \in \mathbb{F}_q$ such that $x^2 = -1$ iff $q \equiv 1 \pmod{4}$ or $q = 2$.*

Proof. If $q = 2$, then $1^2 = 1 = -1$ in $\mathbb{F}_q$.

Otherwise, since the multiplicative group $\mathbb{F}_q^*$ is cyclic there is a $y \in \mathbb{F}_q^*$ which generates it. Then, since its order is $q-1$, by Lemma A.6 we have that

$$-1 = \prod_{n \in \mathbb{F}_q^*} n = y^{\sum_n n} = y^{q(q-1)/2},$$

which is a perfect square iff $q(q-1)/2$ is even; since q is odd, this is the case iff $q-1 \equiv 0(\mathrm{mod} 4)$, or equivalently $q \equiv 1 \pmod 4$. □

References

[1] Ivan Niven. "Formal Power Series". In: *The American Mathematical Monthly* 76.8 (Oct. 1969). Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/00029890.1969.12000359, pp. 871–889. ISSN: 0002-9890. DOI: 10.1080/00029890.1969.12000359. URL: https://doi.org/10.1080/00029890.1969.12000359 (visited on 02/28/2021).