PARTIAL SOLUTIONS TO PRACTICE FINAL

The classics and computational solutions are omitted here.

Problem 1. We are essentially required to solve (reduce) the congruence. We begin by reducing 1111 mod 17. This is done by dividing through by 17 as much as possible, so to speak. More precisely, we make this easier to handle by taking, say, $65 * 17 = 1105$ so that $1111 \cong 6 \bmod 17$. To the exponent we apply Fermat's little theorem. Observe that $2222 = 16 \cdot 138 + 14$ and consequently when taken mod17:

$$1111^{2222} \cong 6^{2222} = 6^{16 \cdot 138} \cdot 6^{14} = \left(6^{16}\right)^{138} \cdot 6^{14} \cong 6^{14}$$

Noting that $6^2 = 36 \cong 2 \bmod 17$ we are left with $2^7 \bmod 17$. Now, $2^6 = 64 \cong 13 \bmod 17$. So that

$$1111^{2222} \cong 2 \cdot 13 = 26 \cong 9 \mod 17$$

Problem 2. It should be intuitively clear that this must hold, and we present a brief proof of this fact. Suppose, by way of contradiction, that instead one has

$$\sqrt{2} + \sqrt{n} \in \mathbb{Q}, \quad \text{for some } n \in \mathbb{N} \tag{1}$$

Note that $n \neq 2$, for in this case we are left with $2\sqrt{2}$ which we know to be irrational. Then, multiplying through by the conjugate will yield

$$\sqrt{n} - \sqrt{2} \cdot \frac{\sqrt{n} + \sqrt{2}}{\sqrt{n} + \sqrt{2}} = \frac{n-2}{\sqrt{n} + \sqrt{2}} \in \mathbb{Q} \tag{2}$$

We know the expression in (2) must be rational since hypothesis the denominator is rational and $n, 2$ are integers. That is, we know that

$$\sqrt{2} + \sqrt{n}, \quad \sqrt{n} - \sqrt{2} \in \mathbb{Q}$$

Subtracting these equations from each other yields $2\sqrt{2} \in \mathbb{Q}$ since $\mathbb{Q}$ is closed under addition (and subtraction). This is absurd.

Problem 3. This is quite an elegant problem. Begin by assuming we may find some $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ so that $x^2 \cong -1 \bmod p$. Since we must have, without a doubt, $(-1)^2 \cong 1 \bmod p$ we may note that since $1^n \cong 1 \bmod p$ for all $n \in \mathbb{N}$:

$$-1 \cong x^2 \cong x^2 \cdot 1 \cong x^2(x^2)^2 \cong x^2\left[(x^2)^n\right] \cong x^{4n+2} \mod p \tag{3}$$

Now recall that $p \cong 3 \bmod 4$. That is, for some $\eta \in \mathbb{Z}$:

$$p = 3 + 4\eta \implies p - 1 = 4\eta + 2 \tag{4}$$

Take now in (3) $n = \eta$ as above in (4). We must have $x^{4\eta+2} = x^{p-1} \cong -1$. However, this is impossible since by *Fermat's Little Theorem* we know this expression must be congruent to 1 modulo p.

Problem 4. Apply the CRT as in the previous assignments. This is a classic.

Problem 5. We shall state the Theorem, despite it being in the notes;

Theorem 1 (CFF)**.** *Let G be a group of finite order and suppose additionally that G acts upon a set S, also of finite order. Let N denote the number of orbits of G in S, then*

$$N = \frac{1}{|G|} \sum_{g \in G} \mathcal{I}(g) \tag{5}$$

where we define

$$\mathcal{I}(g) := |\{s \in S \mid g \star s = s\}|$$

and $|\cdot|$ describes the cardinality of a set.

Proof. We begin by defining a binary mapping $\mathcal{T} : G \times S \to \{0, 1\}$ so that

$$(g, s) \mapsto \begin{cases} 1 & g \star s = s \\ 0 & \text{otherwise} \end{cases}$$

It is important to observe the following:

$$\mathcal{I}(g) = \sum_{s \in S} \mathcal{T}(g, s) \tag{6}$$

$$|\mathrm{Stab}(s)| = \sum_{g \in G} \mathcal{T}(g, s) \tag{7}$$

We recall from a previous result that we may choose a complete set of representatives, say, $(s_k)_{k=1}^N$ for $\mathrm{Orb}(s)$. Then,

$$\begin{aligned}
\sum_{g \in G} \mathcal{I}(g) = \sum_{g \in G} \left(\sum_{s \in S} \mathcal{T}(g, s) \right) &= \sum_{s \in S} \left(\sum_{g \in G} \mathcal{T}(g, s) \right) \\
&= \sum_{s \in S} |\mathrm{Stab}(s)| \\
&= \sum_{s \in S} \frac{|G|}{|\mathrm{Orb}(s)|} \\
&= \sum_{k=1}^{N} \left(\sum_{s \in \mathrm{Orb}(s_k)} \frac{|G|}{|\mathrm{Orb}(s)|} \right) \\
&= \sum_{k=1}^{N} \left(\sum_{s \in \mathrm{Orb}(s_k)} \frac{|G|}{|\mathrm{Orb}(s_k)|} \right) \\
&= |G| \sum_{k=1}^{N} \frac{|\mathrm{Orb}(s_k)|}{|\mathrm{Orb}(s_k)|} \\
&= |G|\,|N|
\end{aligned}$$

which concludes the proof. □

Problem 6.

We begin with a few lemmata; I do not know if these are in the notes (I have not looked). In any case, it is good review.

Lemma 1. *Let G be a cyclic group. Then G is Abelian.*

Proof. Let $g \in G$ be a generator, i.e $G = \langle g \rangle := \{g^n : n \in \mathbb{Z}\}$. Now let $a, b \in G$. We shall show $ab = ba$. Note that we may find a pair $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ so that $g^n = a$ and $g^m = b$. Then,

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$$

which completes the proof. □

Lemma 2. *Let G, H be groups and suppose further that G is cyclic. If $G \cong H$ then H is also cyclic.*

Proof. Let $\varphi : G \to H$ be an isomorphism and choose a generator $g \in G$. We claim that $\varphi(g) =: h$ is a generator for H as well. That is, we must show that for any $f \in H$ we may find an integer n so that $h^n = f$. Indeed, since φ is an isomorphism there exists some $\widetilde{g} \in G$ so that $\varphi(\widetilde{g}) = f$. There is then an integer n so that $g^n = \widetilde{g}$ and therefore

$$f = \varphi(\widetilde{g}) = \varphi(g^n) = \varphi(g)^n$$

which is what we had to show. □

- Take $S_4 < S_6$. This is a subgroup since it is a group itself. The result follows from *Lagrange*'s Theorem.
- Note that S_6 cannot be cyclic by the above. The only possibility is a group H of order 24. If H were cyclic, it would necessarily have an element of order 24.

Problem 7. If we had instead been asked to construct a field of 4 elements, we could have instead presented a table describing operations. However, as this is not trivial to come up with for 16 we are better off (in fact, intended to) construct it using the more general method seen in the notes and lectures. However, this is not *sufficient* to answer the problem, as we are also asked to *prove* that the resulting ring is also a field. Again, with 16 elements this is not easy to verify. We are much better off proving that the method we will use will indeed generate a field, and then apply it to this particular case.

Theorem 2 (From the notes)**.** *Let $\mathbb{F}$ be a field with $p < \infty$ elements. Let $f(x)$ be a non-constant* ***irreducible*** *polynomial over $\mathbb{F}[x]$. The (commutative) ring $\mathbb{F}[x]/(f(x))$ is a field with p^n elements, for $n := \deg f$.*

Proof. We first begin with the observation that $[1] \neq [0]$ in this quotient ring. Indeed, if $1 + (f) = 0 + (f)$ we must also have $1 \in (f)$.

With this out of the way, let $[g(x)] \in \mathbb{F}[x]/(f)$ with $[g(x)] \neq [0]$. We must show that this element has an inverse. To see this, we use that $g(x) \notin (f(x))$ and that f is irreducible to conclude that $\gcd(f, g) = 1$. Hence, by our extended Euclidean Algorithm we may write

$$1 = uf + vg, \quad u(x), v(x) \in \mathbb{F}[x] \tag{8}$$

We now reduce this equation $\mod f$ to observe $1 \cong vg \bmod f(x)$. Thus, $[v(x)]$ is an inverse element for $[g(x)]$ in this quotient ring. Therefore we conclude that $\mathbb{F}[x]/(f(x))$ is indeed a field.

We now show that this field has cardinality p^n. Note that each and every polynomial in $\mathbb{F}[x]/(f(x))$ will have the form (by a class lemma):

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0, \quad a_i \in \mathbb{F}$$

A basic calculation shows that there are exactly p^n such combinations (by cycling through possible coefficients). This completes the proof. □

We now turn our attention to constructing $\mathbb{F}_{16}$ with the help of the above theorem. Recall from the lectures (or notes) that there exists a field with 4 elements, say $\mathbb{F}_4$. This field could be represented as the collection $\{0, 1, a, b\}$ together with the operations:

(9)

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

We need to find an irreducible polynomial over this field. Consider $f(x) = x^2 + x + a$. Indeed,

$$\begin{aligned} 0 &\mapsto a \\ 1 &\mapsto 1 + 1 + a = a \\ a &\mapsto a^2 + a + a = b \\ b &\mapsto b^2 + b + a = b \end{aligned}$$

Since this is quadratic, and has no roots, we conclude $f(x)$ is irreducible over $\mathbb{F}_4$ as required. Then defining

$$\mathbb{F}_{16} := \mathbb{F}_4[x]/(f(x))$$

we conclude by the theorem that this must be a field with $4^2 = 16$ elements.

Problem 8. We will show that $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$. This is nicely done by an application of the *First Isomorphism for Rings*. That is, it is sufficient to find a surjective ring homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{C}$ so that $\ker \varphi = (x^2 + 1)$. This restriction on the kernel of φ is simply the added fact that we require $\varphi = 0 \iff \varphi \in (x^2 + 1)$.

Consider $\varphi : \mathbb{R}[x] \to \mathbb{C}$ defined by $f(x) \mapsto f(\imath)$ where $\imath^2 = -1$. We first show that this mapping fits the kernel criterion. Indeed, it is clear that if $f \in (x^2 + 1)$ then $f(\imath) = 0$. Conversely, suppose that $f \in \ker \varphi$. Then $f(i) = 0$ so that $(x - \imath) \mid f(x)$. But f has real coefficients, so $(x + \imath) \mid f$ as well (this is the *conjugate root theorem*, which we prove below) and hence $(x^2 + 1) \mid f$

It remains to show surjectivity, however this is obvious from the fact that given $\mathbb{C} \ni z = a + bi$ one needs only take

$$\mathbb{R}[x] \ni a + bx \mapsto a + bi$$

Now we show that this is indeed a homomorphism. Clearly the identity elements are preserved, since constants map to constants. As for addition, if $f, g \in \mathbb{R}[x]$ then $\varphi(f + g) = (f + g)(i) = f(i) + g(i)$ and the same argument holds for $f(x)g(x)$.

An application of the *First Isomorphism Theorem for Rings* concludes the exercise.

Now, for the sake of review and completeness we shall provide a proof for the *First Isomorphism Theorem of Rings*.

Theorem 3 (First Isomorphism Theorem for Rings)**.** *Let R, S be rings and suppose $f : R \to S$ is a surjective ring homomorphism. Let $I \lhd R$ and suppose further that $I = \ker f$; denote by $\pi : R \to R/I$ the canonical quotient map. Then $R/I \cong S$.*

Proof. First observe that since $\pi(a+b) = [a+b] = [a] + [b] = \pi(a) + \pi(b)$ and $\pi(ab) = \pi(a)\pi(b)$ whence it is clear that π is indeed a homomorphism of rings. We shall construct an isomorphism $F : R/I \to S$. Consider now such F given by $[a] \mapsto f(a)$. We must first show that this is independent of representative. Indeed, if $[a] = [b] \in R/I$ then these two equivalence classes are equal so that $a - b \in I = \ker f$, thus

$$F([a]) = f(a) = f(a) + f(b-a) = f(a) + f(b) - f(a) = f(b) = F([b])$$

With this out of the way we show that F is an isomorphism of rings. Clearly, $F([1]) = f(1) = 1$ since f is a homomorphism and $F([ab]) = f(ab) = f(a)f(b) = F([a])F([b])$ and similarly for $+$. We claim F is injective, which is seen by noting that $[0] \mapsto 0$ and moreover if $F([a]) = 0$ then $f(a) = 0$ which implies $a \in \ker f = I$ so that $[a] = [0]$. Surjectivity is clear. □

Lemma (Conjugate Root Theorem)**.** *Let $f : \mathbb{C} \to \mathbb{C}$ be a non-constant polynomial with real coefficients. If we have $f(\xi) = 0$ for some $\xi \in \mathbb{C}$ then the complex conjugate $\overline{\xi}$ is also a root of f.*

Proof. We begin by writing $P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + az + a_0$ where $a_k \in \mathbb{R}$ for all $k = 0, 1, \ldots, n$. In particular, $a_k = \overline{a_k}$. Then, since $f(\xi) = 0$:

$$\begin{aligned} 0 = \overline{0} = \overline{f(\xi)} = \overline{\sum_{k=0}^{n} a_k (\xi)^k} = \sum_{k=0}^{n} \overline{a_k (\xi)^k} = \sum_{k=0}^{n} a_k \overline{(\xi)^k} \\ = \sum_{k=0}^{n} a_k \left(\overline{\xi}\right)^k \\ = f\left(\overline{\xi}\right) \end{aligned}$$

Hence $\overline{\xi}$ is also a root of f as was required. Note that such roots are guaranteed to exist by the *Fundamental Theorem of Algebra*, which is a consequence of Liouville's Theorem □

In fact, Liouville's theorem is quite easy to prove provided we accept *Cauchy's Integral Formula*:

Theorem 4. *Let $\Omega \subseteq \mathbb{C}$ be a simply connected domain and let $f : \Omega \to \mathbb{C}$ be holomorphic in this domain. Then, for any closed circle $\gamma \subset \Omega$ so that the interior of γ is also contained in the interior of Ω*

$$f^{(n)}(z) = \frac{n!}{2\pi\imath} \oint_{\gamma} \frac{f(\xi)}{(\xi - z)^{n+1}} \mathrm{d}\xi, \quad \forall z \text{ inside the curve } \gamma \tag{10}$$

Proof. We shall use that f being holomorphic implies that it is also analytic. Fix a point z and expand f as a uniformly convergent power-series in a neighbourhood of z:

$$f(\zeta) = \sum_{n \in \mathbb{N}_0} \frac{f^{(n)}(z)}{n!} (\zeta - z)^n$$

Then, we shall divide through by $(\zeta - z)$ to obtain:

$$\frac{f(\zeta)}{\zeta - z} = \frac{f(z)}{\zeta - z} + \sum_{n=1}^{\infty} \frac{f^{(n)}(z)}{n!} (\zeta - z)^{n-1}$$

Taking the integral over a small circle Γ contained in the integral we have by the uniform convergence of the series:

$$\oint_\Gamma \frac{f(\zeta)}{\zeta - z}\mathrm{d}\zeta = \oint_\Gamma \frac{f(z)}{\zeta - z}\mathrm{d}\zeta + \sum_{n=0}^{\infty} \oint_\Gamma \frac{f^{(n)}(z)}{n!}(\zeta - z)^{n-1}\mathrm{d}\zeta = \oint_\Gamma \frac{f(z)}{\zeta - z}\mathrm{d}\zeta$$

This last integral is exactly:

$$\oint_\Gamma \frac{f(z)}{\zeta - z}\mathrm{d}\zeta = \int_0^{2\pi} \frac{f(z)}{\rho e^{\imath\theta}}\rho e^{\imath\theta}\imath \mathrm{d}\theta = 2\pi\imath f(z)$$

This is the desired result for $n = 0$. Proceed by induction on n to for the general result, which is obvious. □

Remark. Originally I only meant to state this, but instead I ended up proving it too. Whoops.

Lemma. *Let $f : \mathbb{C} \to \mathbb{C}$ be entire (holomorphic in $\mathbb{C}$) and suppose further that for some $n \in \mathbb{N}_0$ one has $f(z) \in \mathcal{O}(z^n)$. Then f is a polynomial of at most degree n.*

Proof. We shall show that $f^{(n+1)} \equiv 0$ in $\mathbb{C}$. Indeed, fix $z \in \mathbb{C}$ and consider a disk C_R centered at z with radius $R \gg 0$. For all sufficiently large R we use the fact that $f(z) \in \mathcal{O}(z^n)$ to see:

$$\begin{aligned}\left|f^{(n+1)}(z)\right| = \left|\frac{n!}{2\pi\imath}\oint_{C_R} \frac{f(\xi)}{(\xi - z)^{n+2}}\mathrm{d}\xi\right| &\leq \frac{1}{2\pi}\oint_{C_R} \frac{|f(\xi)|}{|\xi - z|^{n+2}}\,|\mathrm{d}\xi| \\ &\leq \frac{C}{2\pi}\int_0^{2\pi} \frac{(R + |z|)^n}{R^{n+2}} R\mathrm{d}\theta \xrightarrow{R\to\infty} 0\end{aligned}$$

Thus, we see that $f^{(n+1)}(z) = 0$ and therefore that $f^{(n+1)} \equiv 0$ in $\mathbb{C}$ since z was arbitrary. □

The result when $n = 0$ (i.e f is bounded in constant at infinity) is known as Liouville's theorem:

Theorem 5 (Liouville)**.** *Let $f : \mathbb{C} \to \mathbb{C}$ be entire and suppose there exists a constant $C \geq 0$ so that $|f(z)| \leq C$ in all $\mathbb{C}$, then f is constant.*

Proof. Note that we are given $f \in \mathcal{O}(z^0)$ and thus we have that f is a polynomial of degree 0 by the previous lemma. Hence, f is a constant function. □

The fruit of our labour:

Theorem 6 (The Fundamental Theorem of Algebra)**.** *Let $f : \mathbb{C} \to \mathbb{C}$ be a non-constant polynomial with degree n. Then f has a root in $\mathbb{C}$.*

Proof. By way of contradiction suppose not, then $f(z) \neq 0$ in all $\mathbb{C}$ and hence the quotient $1/f(z)$ is holomorphic in all of $\mathbb{C}$ (entire). Write out now

$$f(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0, \quad a_n \neq 0$$

Whence

$$\frac{f(z)}{z^n} = a_n + \frac{a_{n-1}}{z} + \ldots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}, \quad a_n \neq 0$$

It is clear that $\frac{f(z)}{z^n} \xrightarrow{z\to\infty} a_n$. We may thus find (by definition of the limit) $R \gg 0$ so that for all $|z| > R$:

$$\frac{|f(z)|}{|z|^n} \geq \frac{|a_n|}{2} > 0 \tag{11}$$

Therefore,

$$\left|\frac{1}{f(z)}\right| \leq \left|\frac{2}{z^n a_n}\right| \leq \frac{2}{|a_n|}$$

for all sufficiently large z (i.e $|z| > R$). However, $\frac{1}{f(z)}$ is holomorphic in the compact disk $\{|z| \leq R\}$ and must therefore be bounded there. Hence, $1/f(z)$ is bounded in all of $\mathbb{C}$ and is constant by Liouville's theorem. Contradiction. □

The following theorem is actually pretty dank in my opinion:

Theorem 7. *Let $\mathbb{S}$ denote the Riemann sphere. Then $\mathbb{S}$ is a compact metric space.*

Proof. We shall show that each sequence in $\mathbb{S}$ has a convergent subsequence, which will establish the existence of any open sub-covering. Let $(z_n) \subset \mathbb{S}$ be a sequence. We distinguish several cases:

(1) The sequence is bounded. In this case, we simply view it as a sequence in $\mathbb{C} \subset \mathbb{S}$. Since it is bounded it lives in a compact subset of $\mathbb{C}$ and consequently we may extract a convergent subsequence in $\mathbb{C}$ and hence $\mathbb{S}$.
(2) The sequence is unbounded at finitely many points. In this case, we remove these points at which the sequence is unbounded, and call the resulting subsequence (ζ_n). We may certainly do this, as there are only finitely many $z_n = \infty$. Then we refer to case (1).
(3) There are infinitely many $z_n = \infty$. In this case there is a constant subsequence (ζ_n) so that $\zeta_n = \infty$ for all n. This is a constant sequence in $\mathbb{S}$ and thus is convergent.
(4) The sequence is unbounded with at most finitely many $z_n = \infty$. First edit the sequence to recover a subsequence (ζ_n) so that $\zeta_n \neq \infty$ for all n. Take $M = 1$, there must exist a lowest index $n_1 \in \mathbb{N}$ so that $\zeta_{n_1} > 1$, for otherwise the sequence is bounded. Similarly, take $M = 2$ and find a lowest index $n_2 > n_1$ so that $\zeta_{n_2} > 2$, we must be able to find such an index $n_2 > n_1$ for otherwise as no $\zeta_n = \infty$ we would again have that the sequence was bounded. We proceed in this way, extracting a subsequence (ζ_{n_k}) tending to ∞, and hence converges in $\mathbb{S}$.

□

Remark. I **really** went off on a hell of a tangent there...back to the relevant stuff now.

We give a proof of Cauchy's theorem, despite it not being required

Theorem 8 (Cauchy)**.** *Let G be a group with $|G| = n < \infty$ and let p be a prime dividing n. There exists an element $g \in G$ of order p.*

Proof. Let S be the set of all p-tuples $(g_1, g_2, \ldots, g_p) \in \prod_{i=1}^{p} G$ up to cyclic shifts and denote by T the collection of all p-tuples of the aforementioned sort, distinct. Observe

that S is the set of orbits of T under the action of shifts of $\mathbb{Z}/p\mathbb{Z}$. Hence, we may now apply the CFF formula to deduce that

$$|S| = \frac{n^p - n}{p} + n \tag{12}$$

We claim that $n \nmid |S|$. Otherwise, we would necessarily have $p \mid (n^{p-1} - 1)$ which contradicts $p \mid n$. Define now an action of G on S by taking

$$G \times S \ni (g, s) \mapsto g \star s = (gg_1, gg_2, \dots gg_p)$$

Now, as $n \nmid |S|$ and $|\mathrm{Orb}(s)| = \frac{|G|}{|\mathrm{Stab}(s)|}$ we use the fact that we may write S as the disjoint union of orbits we see that for some s we must have $|\mathrm{Orb}(s)| \neq n$; for otherwise we would have $n \mid |S|$. Therefore for some $s \in S$ we have that $\mathrm{Stab}(s)$ is non-trivial, for otherwise we would again have divisibility.

Fix such s, then for some p-tuple and some i

$$(gg_1, gg_2, \dots, gg_p) = (g_1, g_2, \dots, g_p) \quad \text{up to a cyclic shift} \tag{13}$$

$$(gg_1, gg_2, \dots, gg_p) = (g_{i+1}, g_{i+2}, \dots, g_p, \dots g_1) \tag{14}$$

whence we have $g^p g_1 = g_1$ and hence $g^p = e$. We are done. □