18.781 Solutions to Problem Set 8

1. We know that
$$(1+x)^n = \sum \binom{n}{k} x^k.$$
Now we plug in $x = 1, \omega, \omega^2$ and add the three equations. If $3 \nmid k$ then we'll get a contribution of $1^k + \omega^k + \omega^{2k} = 1 + \omega + \omega^2 = 0$, whereas if $3 \mid k$ we'll get a contribution of $1^k + 1^k + 1^k = 3$. So
$$\begin{aligned}\sum \binom{n}{3k} &= \frac{(1+1)^n + (1+\omega)^n + (1+\omega^2)^n}{3} \\ &= \frac{2^n + (-\omega^2)^n + (-\omega)^n}{3} \\ &= \begin{cases} (2^n+2)/3 & \text{if } n \equiv 0 \pmod 6 \\ (2^n-2)/3 & \text{if } n \equiv 3 \pmod 6 \\ (2^n-1)/3 & \text{if } n \equiv 2,4 \pmod 6 \\ (2^n+1)/3 & \text{if } n \equiv 1,5 \pmod 6 \end{cases}.\end{aligned}$$

2. We have
$$\begin{aligned}\frac{d}{dx}(\tilde{A}(x)) &= \frac{d}{dx}\left(\sum_{n\geq 0} a_n \frac{x^n}{n!}\right) \\ &= \sum_{n\geq 1} a_n \frac{nx^{n-1}}{n!} \\ &= \sum_{n\geq 0} a_{n+1}\frac{x^n}{n!},\end{aligned}$$
which is the exponential generating function of $\{a_1, a_2, \dots\}$.

3. Since c_n is $n!$ times the coefficient of x^n in $\tilde{A}(x)\tilde{B}(x)$,
$$\begin{aligned}c_n &= n!\sum_{k=0}^{n} \frac{a_k}{k!}\cdot\frac{b_{n-k}}{(n-k)!} \\ &= \sum_{k=0}^{n}\binom{n}{k} a_k b_{n-k}.\end{aligned}$$

4. By part (a), $\frac{d}{dx}E(x)$ is the exponential generating function for the sequence $\{r, r^2, r^3, \dots\}$. It follows that $E'(x) = rE(x)$. Since $E(0) = 1$, solving the differential equation, we get
$$E(x) = \sum_{n\geq 0}\frac{r^n x^n}{n!} = e^{rx}.$$

5. (a) In gp, $x/(\exp(x)-1)$ gives the sequence of $B_n/n!$, from which we deduce

n	0	1	2	3	4	5	6	7	8	9	10
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$

(b) First, note that

$$f(x) - f(-x) = \sum_{n \text{ odd}} \frac{2B_n}{n!} x^n.$$

On the other hand,

$$\begin{aligned} f(x) - f(-x) &= \frac{x}{e^x - 1} - \frac{-x}{e^{-x} - 1} \\ &= \frac{x}{e^x - 1} + \frac{xe^x}{1 - e^x} \\ &= \frac{x(1 - e^x)}{e^x - 1} \\ &= -x. \end{aligned}$$

So for $n \geq 3$ odd, $B_n = 0$.

(c) Multiplying both sides of the defining equation by $e^x - 1$, we have

$$x = \left(\sum_{n \geq 0} B_n \frac{x^n}{n!} \right) \left(\sum_{n > 0} \frac{x^n}{n!} \right).$$

For $n \geq 2$, the coefficient of x^n is

$$0 = \sum_{k=0}^{n-1} \binom{n}{k} B_k.$$

(d) We have

$$\begin{aligned} \sum_{k \geq 0} S_k(n) \frac{x^k}{k!} &= \sum_{k \geq 0} (1^k + 2^k + \cdots + n^k) \frac{x^k}{k!} \\ &= e^x + e^{2x} + \cdots + e^{nx} \\ &= e^x \cdot \frac{e^{nx} - 1}{e^x - 1} \\ &= \frac{e^{nx} - 1}{x} \cdot \frac{-x}{e^{-x} - 1} \\ &= \left(\sum_{l=0}^{\infty} \frac{n^{l+1}}{(l+1)!} x^l \right) \left(\sum_{m=0}^{\infty} (-1)^m \frac{B_m}{m!} x^m \right). \end{aligned}$$

Therefore,

$$\begin{aligned} S_k(n) &= k! \sum_{m=0}^{k} \frac{n^{k-m+1}}{(k-m+1)!} \cdot (-1)^m \frac{B_m}{m!} \\ &= \frac{1}{k+1} \sum_{m=0}^{k} \binom{k+1}{m} (-1)^m B_m n^{k+1-m}. \end{aligned}$$

6. (a) If $m = a^2 + b^2$ and $n = c^2 + d^2$, then

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad - bc)^2.$$

Now if $p \equiv 1 \pmod 4$ then p is a sum of two squares (shown in class). If $p \equiv 3 \pmod 4$ then $q^2 = q^2 + 0^2$ is a sum of two squares. Finally, $2 = 1^2 + 1^2$ is a sum of two squares. So any integer of the given form is a sum of two squares.

(b) We want to use induction on n. Assume we have shown that for all integers less than n which are sums of two squares, every prime $p \equiv 3 \pmod 4$ dividing such an integer divides it to an even power. Now suppose $n = a^2 + b^2$ and let $q \equiv 3 \pmod 4$ be a prime dividing n (if there is no such prime, we are done). We claim that q divides a and b. Otherwise, say without loss of generality that $q \nmid b$. Since $a^2 + b^2 = n \equiv 0 \pmod q$, we must have $(ab^{-1})^2 \equiv -1 \pmod q$, which is impossible. This shows that $q \mid a, b$.

Now write $a = a'q$ and $b = b'q$, so that $n = q^2(a'^2 + b'^2)$. Letting $m = a'^2 + b'^2$, by the inductive hypothesis it follows that m is divisible by primes congruent to 3 mod 4 to even powers. Since $n = q^2 m$, n satisfies the same property. With the trivial base case $n = 1$, the induction is complete.

(c) One direction is obvious: if n is a sum of two integer squares, then it's a sum of two rational squares. Suppose now that n is a sum of two rational squares α^2 and β^2. Taking the common denominator, we write $\alpha = a/d, \beta = b/d$. Then $a^2 + b^2 = nd^2$.

Now if we consider any prime $q \equiv 3 \pmod 4$ then q divides $a^2 + b^2$ an even number of times. Obviously q also divides d^2 an even number of times. Therefore, q divides n an even number of times, so n is of the form mentioned in part (b), and is thus a sum of two integer squares.

7. (a) We have

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

Hence $\omega^2 = -\omega - 1$. Now for any complex number $a + b\omega$,

$$\begin{aligned} |a + b\omega|^2 &= (a + b\omega)(\overline{a + b\omega}) \\ &= (a + b\omega)(a + b\omega^2) \\ &= a^2 + b^2 + ab(\omega + \omega^2) \\ &= a^2 - ab + b^2. \end{aligned}$$

So if $M = a^2 - ab + b^2 = |a + b\omega|^2$ and $N = c^2 - cd + d^2 = |d + c\omega|^2$, then

$$\begin{aligned} MN &= |(a + b\omega)(d + c\omega)|^2 \\ &= |ad + bc\omega^2 + (ac + bd)\omega|^2 \\ &= |ad + bc(-\omega - 1) + (ac + bd)\omega|^2 \\ &= (ad - bc)^2 - (ad - bc)(ac + bd - bc) + (ac + bd - bc)^2 \end{aligned}$$

is of the same form.

(b) Suppose $p \equiv 2 \pmod 3$ and $p = a^2 - ab + b^2$. Then $p \nmid a$ or $p \nmid b$, since otherwise $p = a^2 - ab + b^2$ would be divisible by p^2. In fact, if $p|a$ then $p = a^2 - ab + b^2$ implies $p|b^2$, so $p|b$ as well. Thus, p divides neither a nor b. Anyway, $(2a - b)^2 + 3b^2 = 4(a^2 - ab + b^2) \equiv 0 \pmod p$, so

$$\left(\frac{2a - b}{b}\right)^2 \equiv -3 \pmod p.$$

Therefore, -3 is a square mod p. But we've shown before (using quadratic reciprocity) that -3 is a square mod p if and only if $p = 3$ or $p \equiv -1 \pmod 3$, contradiction.

8. (a) For $p = 3$, we have trivially $3 = 1^2 - (1)(-1) + (-1)^2$.

Now suppose $p \equiv 1 \pmod 3$. We'll prove by induction on p that p is of the form $a^2 - ab + b^2$. Assume we have proven this statement for primes less than p. (We can take as our base case $7 = 3^2 - (3)(1) + 1^2$.)

We know -3 is a square mod p, so let x be the solution to $x^2 \equiv -3 \pmod p$, and write $x = 2y - 1$ for some y. Then y satisfies $y^2 - y + 1 \equiv 0 \pmod p$. We can take $|y| < p/2$, so

$$y^2 - y + 1 < \frac{p^2}{4} + \frac{p}{2} + 1 < p^2.$$

Hence $y^2 - y + 1 = np$ for some $n < p$, and we have in addition that $n > 0$ since $y^2 - y + 1 = (y - 1/2)^2 + 3/4 > 0$.

Now let m be the smallest positive integer such that mp can be written in the form $a^2 - ab + b^2$. Note that by the above proof $m < p$, and if $m = 1$ then we are done.

Assume, for the sake of contradiction, that $m > 1$. Let $mp = a^2 - ab + b^2$. We may assume that $g = \gcd(a, b) = 1$, else $g^2 | m$ and thus we can divide a and b by g to reduce m to m/g^2. Now let l be a prime dividing m. Then $l \nmid a$ or $l \nmid b$; say $l \nmid b$. As in Problem 7, we have

$$\left(\frac{2a-b}{b}\right)^2 \equiv -3 \pmod{l},$$

so $l = 3$ or $l \equiv 1 \pmod 3$.

First, suppose $l = 3$. Then we have $a^2 - ab + b^2 \equiv 0 \pmod 3$. Since 3 cannot divide both a and b, it can be easily checked that the only possibility is that $a \equiv 1 \pmod 3$ and $b \equiv -1 \pmod 3$ (or vice versa). Then

$$\left(\frac{a+b}{3}\right)^2 - \left(\frac{a+b}{3}\right)\left(\frac{2a-b}{3}\right) + \left(\frac{2a-b}{3}\right)^2 = \frac{a^2-ab+b^2}{3} = \left(\frac{m}{3}\right)p,$$

so we have a smaller multiple of p, contradiction.

Therefore we must have $l > 3$. Then $x^2 - x + 1 \equiv 0 \pmod l$ for $x \equiv ab^{-1} \pmod l$. Also, since $l \le m < p$, by the inductive hypothesis l is of the form $l = c^2 - cd + d^2$. Again, we can assume that $l \nmid d$, so $y^2 - y + 1 \equiv 0 \pmod l$ for $y \equiv cd^{-1}$.

Now $x^2 - x + 1 \equiv y^2 - y + 1 \pmod l$, so

$$(x-y)(x+y-1) \equiv 0 \pmod{l}.$$

Thus either $x \equiv y \pmod l$ or $x \equiv 1 - y \pmod l$. In the second case, replacing (c, d) by $(d - c, d)$, we note that

$$(d-c)^2 - (d-c)d + d^2 = d^2 - cd + c^2 = l$$

and $(d - c)d^{-1} = 1 - cd^{-1} = 1 - y$, so we may assume that $x \equiv y \pmod l$. It follows that $ab^{-1} \equiv cd^{-1} \pmod l$, so $l \mid ad - bc$.

Now we showed in Problem 7 that

$$(a^2 - ab + b^2)(c^2 - cd + d^2) = (ad - bc)^2 - (ad - bc)(ac + bd - bc) + (ac + bd - bc)^2.$$

The LHS and the first two terms of the RHS are divisible by l. Thus, $l | ad + bd - bc$. Writing $ad - bc = xl$ and $ac + bd - bc = yl$, we now have

$$(mp)(l) = x^2l^2 - xyl^2 + y^2l^2.$$

So

$$\left(\frac{m}{l}\right)p = x^2 - xy + y^2,$$

showing that m is not minimal, contradiction.

Therefore every prime $p \equiv 1 \pmod 3$ can be written in the form $a^2 - ab + b^2$.

(b) One direction is easy: suppose n is positive and every prime $q \equiv 2 \pmod 3$ divides n to an even power. We showed that 3 and primes $p \equiv 1 \pmod 3$ are of the form $a^2 - ab + b^2$. And for $q \equiv 2 \pmod 3$, we have trivially that $q^2 = q^2 - q \cdot 0 + 0^2$ is also of this form. Since the set of numbers of the form $a^2 - ab + b^2$ is closed under multiplication, it follows that n is of the form $a^2 - ab + b^2$ for some integers a, b.

To prove the converse, we first note that if $n = a^2 - ab + b^2$ then

$$n = \left(a - \frac{b}{2}\right)^2 + \left(\frac{b}{2}\right)^2 > 0.$$

(We will exclude the case $a = b = n = 0$.) We now proceed with induction on n. The base case $1 = 1^2 - 1 \cdot 0 + 0^2$ is obvious.

Suppose $q \equiv 2 \pmod 3$ divides $4n$. We claim that $q \mid a, b$. Otherwise, without loss of generality, assume that $q \nmid b$. Then

$$\left(\frac{2a-b}{b}\right)^2 \equiv -3 \pmod q,$$

showing that -3 is a square mod q, which is impossible. So we can write $a = a'q, b = b'q$, and thus $n = q^2(a'^2 - a'b' + b'^2)$. By the inductive hypothesis, q divides $a'^2 - a'b' + b'^2$ to an even power, so it divides n to an even power as well. This completes the induction.

9. Computing,

$$\begin{aligned}
\frac{6157}{783} &= 7 + \frac{676}{783} \\
&= 7 + \cfrac{1}{783/676} \\
&= 7 + \cfrac{1}{1 + \cfrac{107}{676}} \\
&= 7 + \cfrac{1}{1 + \cfrac{1}{676/107}} \\
&= 7 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{34}{107}}} \\
&= 7 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{107/34}}} \\
&= 7 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{5}{34}}}} \\
&= 7 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{34/5}}}} \\
&= [7, 1, 6, 3, 34/5] \\
&= [7, 1, 6, 3, 6, 5/4] \\
&= [7, 1, 6, 3, 6, 1, 4]\,.
\end{aligned}$$

Next,

$$\begin{aligned}
\sqrt{15} &= 3 + \sqrt{15} - 3 \\
&= 3 + \frac{6}{\sqrt{15}+3} \\
&= 3 + \frac{1}{(3+\sqrt{15})/6} \\
&= 3 + \cfrac{1}{1 + \cfrac{\sqrt{15}-3}{6}} \\
&= 3 + \cfrac{1}{1 + \cfrac{1}{6/(\sqrt{15}-3)}} \\
&= 3 + \cfrac{1}{1 + \cfrac{1}{\sqrt{15}+3}} \\
&= 3 + \cfrac{1}{1 + \cfrac{1}{6+\sqrt{15}-3}} \\
&= [3, 1, 6, 1, \dots] \\
&= \left[3, \overline{1, 6}\right].
\end{aligned}$$

10. Taking the log of both sides,

$$\log \sin z = \log z + \sum_{n \geq 1} \log\left(1 - \frac{z^2}{n^2\pi^2}\right).$$

Differentiating,

$$\cot z = \frac{1}{z} + \sum \frac{-\frac{2z}{n^2\pi^2}}{1 - \frac{z^2}{n^2\pi^2}},$$

so

$$\begin{aligned}
z \cot z &= 1 + 2 \sum \frac{z^2}{z^2 - n^2\pi^2} \\
&= 1 - 2 \sum \frac{z^2}{n^2\pi^2} \left(\frac{1}{1 - \frac{z^2}{n^2\pi^2}}\right) \\
&= 1 - 2 \sum \frac{z^2}{n^2\pi^2} \left(\sum_{k \geq 0} \left(\frac{z^2}{n^2\pi^2}\right)^k\right) \\
&= 1 - 2 \sum_{n \geq 1} \sum_{k \geq 1} \frac{z^{2k}}{n^{2k}\pi^{2k}}.
\end{aligned}$$

On the other hand, we have

$$\frac{x}{e^x - 1} = \sum_{r \geq 0} B_r \frac{x^r}{r!},$$

and plugging in $x = 2iz$,

$$\begin{aligned}\sum B_r \frac{(2iz)^r}{r!} &= \frac{2iz}{e^{2iz}-1} \\ &= \frac{2ize^{-iz}}{e^{iz}-e^{-iz}} \\ &= \frac{2iz(\cos z - i\sin z)}{2i\sin z} \\ &= z\cot z - iz.\end{aligned}$$

Taking the real part of this equation, we get

$$\begin{aligned}z\cot z &= \sum_{\substack{r\geq 0 \\ r \text{ even}}} B_r \frac{(2i)^r}{r!} z^r \\ &= \sum_{k\geq 0} B_{2k} \frac{(-1)^k 2^{2k}}{(2k)!} z^{2k} \\ &= 1 - \sum_{k\geq 1} (-1)^{k-1} \frac{B_{2k} 2^{2k}}{(2k)!} z^{2k}.\end{aligned}$$

Equating the two expressions, and taking the coefficient of z^{2k},

$$(-1)^{k-1} \frac{B_{2k} 2^{2k}}{(2k)!} = \frac{2}{\pi^{2k}} \sum_{n\geq 1} \frac{1}{n^{2k}}.$$

So we conclude that

$$\zeta(2k) = \sum_{n\geq 1} \frac{1}{n^{2k}} = (-1)^{k-1} B_{2k} \frac{2^{2k-1}}{(2k)!} \pi^{2k}.$$