Hints for exercises in chapter 5

Exercise 5.1.4. Show that if $2^{2^{n-1}} < x \le 2^{2^n}$, then there are $\ge n$ primes up to x. Then give a lower bound for n as a function of x.

Exercise 5.3.2. Show that if every prime factor of n is $\equiv 0$ or $1 \pmod 3$, then $n \equiv 0$ or $1 \pmod 3$.

Exercise 5.3.4. Consider splitting arithmetic progressions mod 3 into several arithmetic progressions mod 6.

Exercise 5.3.5. One might use exercise 3.1.4(b) in this proof.

Exercise 5.4.1(b). We wish to show that $\pi(x+\epsilon x) > \pi(x)$. By (5.4.2) (and footnote 14) we know that for any fixed $\delta > 0$ we have $(1-\delta)\frac{x}{\log x} < \pi(x) < (1+\delta)\frac{x}{\log x}$ if x is sufficiently large. The result will then follow if the middle inequality holds in

$$\pi(x) < (1+\delta)\frac{x}{\log x} < (1-\delta)\frac{x+\epsilon x}{\log(x+\epsilon x)} < \pi(x+\epsilon x).$$

Now $\frac{\log(x+\epsilon x)}{\log x} < 1 + \frac{\epsilon}{\log x}$ as $\log(1+\epsilon) < \epsilon$, and so the middle inequality follows if $1 + \frac{\epsilon}{\log x} < (1-\delta)(1+\epsilon)/(1+\delta)$. Selecting, say, $\delta = \epsilon/3$ this holds if x is sufficiently large.

Exercise 5.8.11. Use l'Hôpital's rule.

Exercise 5.8.12. First prove that $\left(\mathrm{Li}(x) - \frac{x}{\log x}\right) \Big/ \frac{x}{(\log x)^2} \to 1$ as $x \to \infty$.

Exercise 5.8.14(a). Use Corollary 2.3.1.

Exercise 5.9.1. Either use Kummer's Theorem (Theorem 3.7) or consider directly how often p divides the numerator and denominator of $\binom{2n}{n}$.

Exercise 5.9.3. Use induction to show that, for each $n \ge 6$, every integer in $[7, 2N+6]$ is the sum of distinct primes in $\{2, 3, \dots, 2N\}$, by induction on $N \ge 1$.

Exercise 5.9.6. Let p be a prime in $[2n, 4n]$. Now construct all the pairs you can that sum to p. Proceed.

Exercise 5.10.1. Maximize the log of the ratio using calculus.

Exercise 5.10.2. Use Proposition 5.10.1.

Exercise 5.10.3(a). If $r \le s/2$, then by Bertrand's postulate there is a prime $p \in (s/2, s] \subset (r, s]$. Otherwise $k = s - r \le r$. In either case, by Bertrand's postulate or the Sylvester-Schur Theorem, one term has a prime factor $p > k$, and so this is the only term that can be divisible by p.

Exercise 5.11.8(b). Use the Fundamental Theorem of Algebra mod p (see Lagrange's Theorem, Proposition 7.4.1).

Exercise 5.11.9(a). Can be proved by induction on k. For $k = 0$ this is trivial. For larger k, let $T \subset \{1, 2, \dots, m-1\}$ and we pair together the terms for $S = T$ and

$S = T \cup \{m\}$ in our sum. The sum therefore becomes

$$\sum_{T\subset\{1,2,\dots,m-1\}} (-1)^{|T|} \left(\left(x_m + x_0 + \sum_{j\in T} x_j \right)^k - \left(x_0 + \sum_{j\in T} x_j \right)^k \right)$$
$$= \sum_{i=0}^{k-1} \binom{k}{i} x_m^{k-i} \sum_{T\subset\{1,2,\dots,m-1\}} (-1)^{|T|} (x_0 + \sum_{j\in T} x_j)^i$$

and the result follows by induction, as $m - 1 > k - 1 \geq i$.

(b) Let $x_0 = \log n$ and if n has prime factors $p_1, \dots, p_m$, then let $x_j = -\log p_j$ for each $j \geq 1$.

(c) We get $k! x_1 \dots x_k$ in (a) and so $(-1)^k k! \prod_{p|n} \log p$ in (b). We prove this by induction using the proof in (a), since in the induction step only the $i = k-1$ term remains, which is the result from the previous step multiplied by kx_k.

Exercise 5.16.1. If $\mathrm{Re}(s) > 1$, then the Euler product for $\zeta(s)$ is absolutely convergent (as we proved) and so $\zeta(s) = 0$ if and only if some $1 - p^{-s} = 0$.

Exercise 5.28.3. We will show how to find all the possible orbits when the period has length 1:

(a) Suppose we have the orbit $0 \to b \to a \to a \to \cdots$ with $0, a, b$ distinct integers. By Corollary 2.3.1, we have that $b = b - 0$ divides $f(b) - f(0) = a - b$ and so b divides a. Moreover, $a = a - 0$ divides $f(a) - f(0) = a - b$ and so a divides b. Therefore $|b| = |a|$, and so $b = -a$ as a and b are distinct. To find the polynomials $f(.)$ for which $f(0) = -a, f(a) = f(-a) = a$ we extrapolate. The second two conditions give that $f(x) = a + (x - a)(x + a)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Substituting in $x = 0$ gives $-a = f(0) = a - a^2 h(0)$, so that a^2 divides $2a$; that is, $a = -2$, -1, 1, or 2 (as $a \neq 0$).

(b) Can an orbit have the shape $0 \to u \to v \to w \to w \to \cdots$ with $0, u, v, w$ distinct integers? Let $g(x) = f(x + u) - u$ so that this orbit becomes $-u \to 0 \to b \to a \to a \to \cdots$ where $b = v - u$ and $a = w - u$. Then $b = -a = -2$, -1, 1, or 2 by (a). By Corollary 2.3.1, we have $u = 0 - (-u)$ divides $b - 0 = -a$ and so $u = \pm 1$ and $a = \pm 2$. Next $b + u = u - a$ divides $a - 0 = a$ and so $a = 2u$, which is impossible or else $a - (-u) = 3u$ divides $a - 0 = 2u$.

Exercise 5.28.4(c). If x_0 is periodic, then $x_{n+2} = x_n$ for all $n \geq 0$ as the period length is either one or two. Moreover, if x_0 is strictly preperiodic, then 0 is strictly preperiodic for the map $x \to f(x + x_0) - x_0$, with orbit $0 \to b_1 \to b_2 \to \cdots$ where $b_n = x_n - x_0$. In all four cases of our classification $b_2 = b_4$, and so $x_2 = x_4$.

Hints for exercises in chapter 6

Exercise 6.1.2. Study where lines of rational slope, going through the point $(2, 1)$, hit the curve again.

Exercise 6.1.5. Write down an equation that identifies when three given squares are in arithmetic progression.

Exercise 6.3.1(a). By (6.1.1) the area is $g^2rs(r^2-s^2)$ where $r > s \geq 1$ and $(r, s) = 1$. If this is a square, then each of r, s, and $r^2 - s^2$ must be squares; call them x^2, y^2, and z^2, respectively, so that $x^4 - y^4 = z^2$, which contradicts Theorem 6.2.

(c) Consider a right-angled triangle with sides $x^2, 2y^2, z$.

Exercise 6.5.3. Here b is the hypotenuse, and c is the area. Further hint: We need $b^2 - 4c$ and $b^2 + 4c$ to be integer squares, say, u^2 and v^2, so that $4c = b^2 - u^2 = v^2 - b^2$. Therefore $2b^2 = u^2 + v^2$, so u, v have the same parity and therefore $(\frac{u+v}{2})^2 + (\frac{u-v}{2})^2 = b^2$. This is our Pythagorean triangle, which has area $\frac{1}{2} \cdot \frac{u+v}{2} \cdot \frac{v-u}{2} = \frac{v^2-b^2+b^2-u^2}{8} = c$.

Exercise 6.5.6. Let $\alpha = p/q$ with $(p, q) = 1$ so that $\alpha = (a\alpha + b)/\alpha = (ap + bq)/p$. Now $(p, q) = 1$ so comparing denominators we must have $q = 1$, and p divides $ap + bq$, so that p divides bq, and therefore b.

Exercise 6.5.7. By (6.1.1) the perimeter of such a triangle has length $2grs + g(r^2 - s^2) + g(r^2 + s^2) = 2gr(r + s)$ where $r > s > 0$. Therefore n has divisors r and $r + s$, where $r < r + s < 2r$. On the other hand if n has divisors d_1, d_2 for which $d_1 < d_2 < 2d_1$, then we may assume they are coprime, by dividing through by any common factor. Therefore d_1d_2 divides n and so we can let $r = d_1$, $s = d_2 - d_1$, and $g = n/d_1d_2$.

Exercise 6.5.9. Prove that if $n \geq 13$, then $(n + 1)^2 + 128 < 2n^2$. Then proceed by induction on n for $m \in [n^2 + 129, 2n^2)$.

Exercise 6.5.10. What values can cubes take mod 9?

Exercise 6.8.1. By simple geometry things must look like the following diagram.

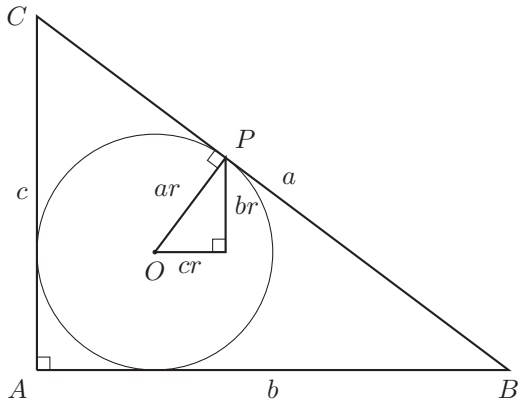

Figure. A circle inscribed inside a right-angled triangle.