Midterm Solutions

by Pinar Colak

(1) By Chebyshev's Theorem, we know that there exists two positive real numbers α and β such that

$$\frac{\alpha x}{\log x} < \pi(x) < \frac{\beta x}{\log x}.$$

Let $x = p_n$, that is, the n^{th} prime number, then $\pi(p_n) = n$, and the inequality becomes

$$\frac{\alpha p_n}{\log p_n} < n < \frac{\beta p_n}{\log p_n}$$

or in other words,

$$\alpha p_n < n \log p_n < \beta p_n. \qquad (*)$$

Note that $n < p_n$, and this implies that $\log n < \log p_n$. The inequality (*) implies

$$n \log p_n < \beta p_n$$
$$\implies \frac{1}{\beta} n \log p_n < p_n$$
$$\implies \frac{1}{\beta} n \log n < p_n.$$

Taking $a = \frac{1}{\beta}$ gives the claimed lower bound $an \log n < p_n$.

For the upper bound, we first recall the fact that $\log x < \sqrt{x}$ for $x \geqslant 1$. Plugging this into (*) gives

$$\alpha p_n < n \log p_n < n\sqrt{p_n}.$$

Thus,

$$\sqrt{p_n} < \frac{n}{\alpha}$$
$$\implies \frac{1}{2} \log p_n < \log n - \log \alpha$$
$$\implies \log p_n < 2 \log n - 2 \log \alpha$$
$$\implies \alpha p_n < n \log p_n < 2n \log n - 2n \log \alpha$$
$$\implies p_n < \frac{2n \log n - 2n \log \alpha}{\alpha} = \frac{2 - 2\frac{\log \alpha}{\log n}}{\alpha}(n \log n).$$

Note that $\log \alpha$ might be negative, so we cannot just take $b = \frac{2}{\alpha}$. However, the more complicated choice $b = \dfrac{2 + 2\left|\frac{\log \alpha}{\log 2}\right|}{\alpha}$ does the trick: $p_n < bn \log n$ for all $n \geqslant 2$.

(2) There exists some integer a such that $a \leqslant x < a + 1$ (so $[x] = a$). It follows that $2a \leqslant 2x < 2a + 2$, whence $[2x] = 2a$ or $2a + 1$. Thus

$$[2x] - 2[x] = (2a \text{ or } 2a + 1) - 2a = 0 \text{ or } 1.$$

(3) (a) We have

$$\begin{aligned} 13! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \\ &= 2^{10} \cdot 3^5 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13. \end{aligned}$$

We get that $\mathrm{ord}_2(13!) = 10$ and $\mathrm{ord}_3(13!) = 5$.

(b) First, observe that

$$\mathrm{ord}_p(m) = \sum_{\substack{k \geqslant 1 \\ \text{s.t.} \\ p^k | m}} 1$$

Thus, we have

$$\begin{aligned} \mathrm{ord}_p(n!) &= \sum_{m \leqslant n} \mathrm{ord}_p(m) = \sum_{m \leqslant n} \sum_{\substack{k \geqslant 1 \\ \text{s.t.} \\ p^k | m}} 1 \\ &= \sum_{k \geqslant 1} \sum_{\substack{m \leqslant n \\ \text{s.t.} \\ p^k | m}} 1 = \sum_{k \geqslant 1} \sum_{d \leqslant \frac{n}{p^k}} 1 \qquad (\text{writing } m = p^k d) \\ &= \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor. \end{aligned}$$

Note that $2^n \geqslant n$ for all $n \in \mathbb{N}$. It follows that for all $k > n$, we have

$$p^k > p^n \geqslant 2^n \geqslant n.$$

Thus, for all $k > n$, we have $0 \leqslant \frac{n}{p^k} < 1$, i.e. $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. We conclude that

$$\mathrm{ord}_p(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{n} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

(c) First rewrite

$$\mathrm{ord}_p \binom{2n}{n} = \mathrm{ord}_p(\frac{(2n)!}{(n!)^2}).$$

By using the rules of $\mathrm{ord}_p(n)$ we can write

$$\begin{aligned} \mathrm{ord}_p(\frac{(2n)!}{(n!)^2}) &= \mathrm{ord}_p((2n)!) - \mathrm{ord}_p((n!)^2) \\ &= \mathrm{ord}_p((2n)!) - 2\mathrm{ord}_p(n!). \end{aligned}$$

By using part (b), we get

$$= \sum_{k=1}^{2n} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \sum_{k=1}^{n} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Note that $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ whenever $p^k > n$. This is the case for $k = n+1, \cdots, 2n$, hence

$$\sum_{k=n+1}^{2n} \left\lfloor \frac{n}{p^k} \right\rfloor = 0.$$

So subtract twice of it from the previous equality:

$$\begin{aligned} &= \sum_{k=1}^{2n} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\sum_{k=1}^{n} \left\lfloor \frac{n}{p^k} \right\rfloor - 2\sum_{k=n+1}^{2n} \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= \sum_{k=1}^{2n} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\sum_{k=1}^{2n} \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= \sum_{k=1}^{2n} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right). \end{aligned}$$

Let $m = \mathrm{ord}_p((2n!))$, which means that $p^m | (2n!)$. This implies that $p^m < 2n$, which can be rewritten as $m < \frac{\log(2n)}{\log p}$, hence $\left\lfloor \frac{2n}{p^k} \right\rfloor$ gives 0 for all $k > \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor$. By using this, we can rewrite the equality above as

$$= \sum_{k=1}^{\left\lfloor \frac{\log(2n)}{\log p} \right\rfloor} (\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor).$$

By using M2, we know that each term inside this sum is either 1 or 0. Hence the total sum is less then or equal to

$$\left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \leqslant \frac{\log(2n)}{\log p} = \frac{\log n}{\log p} + \frac{\log 2}{\log p} \leqslant \frac{\log n}{\log p} + 2.$$

(4) Since $p \geqslant 5$, we see that $(p, 3) = 1$. Fermat's Little Theorem immediately implies that $p^2 \equiv 1 \pmod 3$. In other words,

$$3 \mid p^2 - 1.$$

Since p is odd, we see that $(p, 8) = 1$, whence $p \in \mathbb{Z}_8^\times$. As we have seen in lecture, $n^2 = 1$ for all $n \in \mathbb{Z}_8^\times$; it follows that

$$8 \mid p^2 - 1.$$

Finally, by Problem 1.9(i) from the first problem set, we conclude that $24 \mid p^2 - 1$.

(5) First we will rewrite $n^4 + n^2 + 1$ to factorize it:

$$\begin{aligned} n^4 + n^2 + 1 &= n^4 + n^2 + 1 + n^2 - n^2 = n^4 + 2n^2 + 1 - n^2 \\ &= (n^2+1)^2 - n^2 = (n^2 - n + 1)(n^2 + n + 1). \end{aligned}$$

If $n^4 + n^2 + 1$ is a prime number, then its only factors are 1 and itself, hence either $n^2 - n + 1$ or $n^2 + n + 1$ is 1. Since $n^2 + n + 1$ is always greater than 3 if n is a natural number, so we get that $n^2 - n + 1$ has to be 1. Let's solve for n:

$$\begin{aligned} n^2 - n + 1 &= 1 \\ n^2 - n &= 0 \\ n(n-1) &= 0, \end{aligned}$$

hence either $n = 0$ or $n = 1$. It is given that n is a natural number, so $n \neq 0$. The only possible n such that $n^4 + n^2 + 1$ is prime is $n = 1$. In this case we get $1 + 1 + 1 = 3$, which is indeed a prime number. So the list consists of only $n = 1$.

(6) (a) Since $(A, B) = 1$, we know that there exist integers x' and y' such that

$$Ax' + By' = 1.$$

Multiply both sides by C:

$$\begin{aligned} ACx' + BCy' &= C \\ Ax + By &= C, \end{aligned}$$

where $x = Cx'$ and $y = Cy'$.

(b) We will prove a stronger result (given by David Salwinski on his midterm): if $C > AB$, then there exist positive integer solutions. From part (a), we know that we can find integers x' and y' such that $Ax' + By' = C$. Note that

$$Ax' + By' = C > AB,$$

since both A and B are positive. Divide both sides by AB:

$$\begin{aligned} \frac{x'}{B} + \frac{y'}{A} &> 1 \\ \frac{y'}{A} - (-\frac{x'}{B}) &> 1. \end{aligned}$$

This implies that the length of the interval $(-\frac{x'}{B}, \frac{y'}{A})$ is greater than 1, so there must be an integer K lying in it. Then we get $-\frac{x'}{B} < K$ which gives $x' + KB > 0$, and $\frac{y'}{A} > K$ which gives $y' - KA > 0$. Finally, we show that these two positive integers satisfy the given equation:

$$\begin{aligned} A(x' + KB) + B(y' - KA) &= Ax' + KAB + By' - KAB \\ &= Ax' + By' = C. \end{aligned}$$