m3pm16soln2.tex

M3PM16/M4PM16 SOLUTIONS 2. 29.1.2015

Q1.

$$\exp\{(\log x)^a\} = \sum_{n=0}^{\infty} (\log^a x)^n / n! = \sum_0^{\infty} (\log^{na} x)/n!$$

For any power $\log^k x$ of $\log x$, taking n so large that $na > k$ and letting $x \to \infty$ gives

$$\exp\{(\log x)^a\}/\log^k x \to \infty.$$

But $\log^a x < \log x$ as $a < 1$, so

$$\exp\{(\log x)^a\}/\exp\{\log x\} = \exp\{(\log x)^a\}/x \to 0.$$

Q2. (i) Then either form of remainder given is smaller than $O(x/\log^k x)$, so gives a better result in PNT.
(ii) Knowing that PNT with error term as in IV.5 is available, this shows that it is simpler to use $li(x)$ throughout than $x/\log x$ or any of its logarithmic refinements.

To summarise: with PNT, $\pi(x) \sim li(x) \sim x/\log x$, $li(x)$ and $x/\log x$ are equivalent, and it doesn't matter which we use. In PNT with remainder: in IV.5 we prove $\pi(x) = li(x) + O(xe^{-\sqrt{c \log x}})$. This lovely classical remainder term is destroyed if we replace $li(x)$ by $x/\log x$ with error term $O(x/\log^2 x)$ (or refinements such as $x/\log x + x/\log^2 x + \ldots + (m-1)!x/\log^m x$ with error term $O(x/\log^{m+1})$).

It is nevertheless worth knowing – and highly non-trivial – that

$$\pi(x) = x/\log x + O(x/\log^2 x).$$

It seems that there is no quicker way of proving this seemingly crude form of PNT with remainder except by specialisation of the classical result. See e.g. IV.5 L32.

Q3. If $n = 0$, take $x = y = 0$. So assume $n > 0$.
If (a, b) does not divide n, there is no solution ((a, b) divides LHS but not RHS).
If (a, b) divides n: by the Euclidean Algorithm, there are integers c, d with

$$ac + bd = (a, b).$$

So

$$a(\frac{nc}{(a,b)}) + b(\frac{nd}{(a,b)}) = n,$$

and as $(a,b)|n$, $(a,b)m = n$ say, this says

$$a(mc) + b(md) = n,$$

giving the required solution. //

Q4. As $(a,b) = 1$, there are integers m, n with

$$am + bn = 1,$$

by the Euclidean Algorithm. So

$$acm + bcn = c.$$

But $a|bc$, so $a|$LHS. So $a|$RHS, i.e. $a|c$. //

Q5 (HW, Th. 3, who call this 'Euclid's first theorem'). Take $p = a$ in Q4, and then replace b, c by a, b. Then $p|a$ unless $(p,a) = 1$, and then $p|b$ by Q4.

Q6. If there are only finitely many primes, list them as $p_1, \ldots, p_n$. Then

$$q := 1 + p_1 p_2 \ldots p_n$$

is not divisible by any p_i $(i = 1, \ldots, n)$ – it has remainder 1. But by FTA, q is a product of the primes, $p_1, \ldots, p_n$. This is a contradiction.
(ii) Ordinary Mathematics allows proof by contradiction (Example: $\mathbb{N}$ is infinite – for if it had a largest member, n, $n + 1$ would be bigger) – though Intuitionism, a branch of Mathematical Logic, does not allow proof by contradiction.

In general, prefer a direct proof to one by contradiction: "Inside every proof by contradiction, there is a direct proof struggling to get out". This view is convincingly argued in the lovely and highly informative book
George PÓLYA, *How to solve it*, 2nd ed., Doubleday, 1957.

In this spirit, one could rephrase the proof that $\mathbb{N}$ is infinite positively, as in L1: start with $n = 1$ and keep adding 1; this process never ends, so $\mathbb{N}$ never ends – is infinite (without end – this is what the word means; cf. fin = end, in French: the last frame of a French film consists of the word FIN).

NHB