Example Answers to the Elementary Number Theory Exam held on 2-feb-2006

Question 1. *(a) Determine all $x \in \mathbb{Z}$ that simultaneously satisfy*

$$\begin{aligned} x &\equiv 2 (\bmod \bmod 11), \\ 7x &\equiv 4 (\bmod \bmod 12), \\ x &\equiv 4 (\bmod \bmod 13). \end{aligned}$$

(b) Show that the pair of congruence relations

$$x \equiv a_1 (\bmod \bmod m_1), \qquad x \equiv a_2 (\bmod \bmod m_2) \tag{1}$$

has a solution iff $\gcd(m_1, m_2)$ *divides* $a_1 - a_2$.

Answer. (a) By the Chinese Remainder theorem (CRT) there is a unique solution modulo $11 \cdot 12 \cdot 13$. The value will be deduced by repeated applications of the CRT.

Multiplying the 2nd equation through by 7 (which is invertible mod 12), we see that the 2nd equation is equivalent to $x \equiv 4 (\bmod 12)$. By the CRT, there is a unique x modulo $12 \cdot 13$ that solves both $x \equiv 4 (\bmod 12)$ and $x \equiv 4 (\bmod 13)$. It must be the obvious solution $x \equiv 4 (\bmod 12 \cdot 13)$. Therefore we have reduced our task to solving

$$\begin{aligned} x &\equiv 2 (\bmod \bmod 11), \\ x &\equiv 4 (\bmod \bmod 12 \cdot 13). \end{aligned}$$

But x satisfies the second of these equations if we can write $x = 12 \cdot 13n + 4$ for some $n \in \mathbb{Z}$. Furthermore $12 \cdot 13n + 4 \equiv 2 (\bmod 11)$ if and only of $n \equiv -1 (\bmod 11)$. Hence $n = -1 + 11k$ and $x = -152 + 11 \cdot 12 \cdot 13k$. The solution is given by the residue class $-151 (\bmod 11 \cdot 12 \cdot 13)$.

(b) Let $d := \gcd(m_1, m_2)$. If $\exists\, x$ so that (1) then clearly $x \equiv a_1 (\bmod d)$ and $x \equiv a_2 (\bmod d)$. Taking the difference we get $0 \equiv a_1 - a_2 (\bmod d)$ and so d divides $a_1 - a_2$.

It remains to prove the converse.

To see this note that there are $b_1, b_2 \in \mathbb{Z}$ so that

$$d = -b_1 m_1 + b_2 m_2. \tag{2}$$

hence if $a_1 - a_2 = \lambda d$ for some $\lambda \in \mathbb{Z}$ then

$$a_1 - a_2 = -\lambda b_1 m_1 + \lambda b_2 m_2.$$

Therefore

$$x := a_1 + \lambda b_1 m_1 = a_2 + \lambda b_2 m_2$$

is well defined and provides a solution to (1). □

Question 2. *(a) Suppose x is an odd number. Show that every prime divisor p of x^2+4 satisfies $p \equiv 1 \mod 4$. Show also that at least one of the prime divisors p satisfies $p \equiv 5 \mod 8$.*

(b) Deduce that there are an infinite number of primes of the form 5 mod 8.

Answer. (a) As x is odd any prime divisor p is odd. Also $p|x^2+4$ implies that $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = -1$. We deduce by [1], Corollary 11.1.5, that $p \equiv 1 (\text{mod } 4)$. If all the prime divisors were $1(\text{mod mod } 8)$, then $x^2+4 \equiv 1(\text{mod mod } 8)$ also, and so $x^2 \equiv 5(\text{mod mod } 8)$. However odd integers squared are always $1(\text{mod mod } 8)$ (proof: expand $(4m \pm 1)^2$). Therefore there must be a prime divisor p with $p \equiv 5(\text{mod mod } 8)$.

(b) Suppose $p_1, \dots, p_m$ lists all primes of the form $5(\text{mod mod } 8)$. Let $x := \prod_{i=1}^m p_i$. By part (a), x^2+4 has a prime divisor p with $p \equiv 5((\text{mod mod } 8))$. As p already occurs among the p_i we get that p divides 4. This is impossible. Conclusion: there are an infinite number of primes of the form $5(\text{mod mod } 8)$. □

Question 3. *Find all integers x, y, z with* $\gcd(x, y) = 1$ *and*

$$z^2 = xy(x+y). \tag{3}$$

Answer. Note: There was a misprint in the exam, there it was asked that $\gcd(x, y, z) = 1$.

We claim that there are coprime integers s, t of different parity so that after possibly swapping x with y one of the following is true.

- $(x, y, z) = \big((s^2-t^2)^2,\ (2st)^2,\ \pm 2st(s^4-t^4)\big)$,
- $(x, y, z) = \big((s^2-t^2)^2,\ -(s^2+t^2)^2,\ \pm 2st(s^4-t^4)\big)$,
- $(x, y, z) = \big((2st)^2,\ -(s^2+y^2)^2,\ \pm 2st(s^4-t^4)\big)$,
- (x, y, z) is one of $(0, \pm 1, 0), (1, -1, 0)$.

In the exam we would have been happy if one of the above parametrisations were found by the student. Now on with the solution.

We see that x, y cannot both be negative. Therefore, after swapping x, y, solutions will all fall into one of the 3 cases discussed below. The combined discussions prove the claim.

Case 1. $z \neq 0, x > 0, y > 0$.

By the unique factorization of integers, there are non-zero integers a, b, c so that $x = a^2, y = b^2, x + y = c^2$. As $\gcd(x, y) = 1$, a, b are coprime and satisfy $a^2 + b^2 = c^2$. I.e. (a, b, c) are a *Pythagorian Triple* (see [1], Definition

31.1.1). Theorem 13.1.2 of [1] implies after possibly swapping x with y, that there are coprime integers s, t of different parity so that

$$x = (s^2 - t^2)^2, \quad y = (2st)^2, \quad z = \pm 2st(s^4 - t^4).$$

Case 2. $z \neq 0, x > 0, y < 0$.

Now there is a Pythagorian Triple (a, b, c) so that $x = a^2, y = -c^2, x+y = -b^2$. Arguing as in case 1, that there are coprime integers s, t of different parity so that either

$$x = (s^2 - t^2)^2, \quad y = -(s^2 + t^2)^2, \quad z = \pm 2st(s^4 - t^4).$$

or

$$x = (2st)^2, y = -(s^2 + t^2)^2, z = \pm 2st(s^4 - t^4).$$

Case 3. $z = 0$.

If $z = 0$ we see that after possibly swapping x with y that (x, y, z) is one of $(0, \pm 1, 0), (1, -1, 0)$.

□

Question 4. *Assume that the abc-conjecture holds. Suppose A, B, p, q are fixed positive integers with $p, q \geq 2$ and $pq > 4$. Show that there are only a finite number of positive integers x, y such that*

$$Ax^p - By^q \;=\; 2. \tag{4}$$

Answer. For the definition of $\text{Rad}(n)$ and a statement of the *abc*-conjecture see [1][chapter 17]. Note: We would have been happy if you had done the problem correctly under the assumption that $\gcd(Ax^p, By^q, 2) = 1$. Here is the complete solution.

Set $a := 2/d, b := By^q/d, c := Ax^p/d$, where $d = \gcd(2, By^q, Ax^p)$. Now a, b, c are a triple of *coprime* positive integers with $a + b = c$. We will apply the *abc*-conjecture to this triple with an $\epsilon > 0$ that we will specify later. The assumed conjecture implied that

$$c \leq (\text{Rad}(abc))^{1+\epsilon}. \tag{5}$$

with finitely many exceptions. From the definition of Rad,

$$\begin{aligned} \text{Rad}(abc) &\leq \text{Rad}(d^3abc) \\ &= \text{Rad}(2ABx^py^q) \\ &\leq 2ABxy. \end{aligned}$$

Furthermore equation (4) implies that $y^q \leq A/Bx^p$, so that certainly $y \leq Ax^{\frac{p}{q}}$. Hence

$$\text{Rad}(abc) \;\leq\; 2ABx^{p(\frac{1}{p}+\frac{1}{q})}. \tag{6}$$

Combining (5) and (6) gives

$$Ax^p/d \leq \left(2ABx^{p(\frac{1}{p}+\frac{1}{q})}\right)^{1+\epsilon}.$$

Since $p, q \geq 2$ and $pq > 4$ we find that $\frac{1}{p} + \frac{1}{q} \leq \frac{1}{2} + \frac{1}{3} = \frac{5}{6}$. Also $d \leq 2$, so that

$$x^p \leq \frac{2}{A}\left(2ABx^{\frac{5}{6}p}\right)^{1+\epsilon}.$$

We now know choose $\epsilon = 1/10$ to get

$$\begin{aligned} x^{\frac{1}{12}p} &\leq \frac{2}{A}(2AB)^{1.1} \\ &\leq 8AB^2. \end{aligned}$$

Hence

$$x \leq x^p \leq (8AB^2)^{12}.$$

Therefore, there is an upper bound on the value of x. Equation (4) now implies a bound on y also. Hence there are only finitely many positive integer x, y that satisfy (4). □

Question 5. *(a) Show that $\pi(n) < \frac{n}{3} + 2$ for all positive integers, where $\pi(n)$ is the prime number function.*

(b) Show that there is a sequence of positive integers $n_1, n_2, n_3 \dots$ so that $\phi(n_k)/n_k \to 0$ as $k \to \infty$.

(c) Show that $\pi(n)/n \to 0$ as $n \to \infty$.

Answer. For the definitions of $\pi(n)$ and $\phi(n)$ see [1], chapters 7 and 19.

(a) By inspection the inequality is true for $n = 1, \dots, 6$. In every sequence of 6 consecutive integers at most 2 can be prime. This is because if $m \equiv 0, 2, 3, 4(\text{mod mod } 6)$ then m must be composite. Therefore, if the inequality holds for n, it holds for $n + 6$. It now follows by induction that the inequality holds for all positive integers.

(b) For this we define $n_k = \prod_{i=0}^{k} p_i$ where p_i denotes the i-th prime. Showing that $\phi(n_k)/n_k \to 0$ is equivalent to showing that $n_k/\phi(n_k) \to \infty$.

Using the formula for $\phi(n)$ given in [1], Theorem 7.1.1, we get

$$\begin{aligned}
\frac{n_k}{\phi(n_k)} &= \prod_{i=0}^{k}\left(1-\frac{1}{p_i}\right)^{-1} \\
&= \sum_{m>0,\ \text{divisible only by } p_1,\ldots,p_k} \frac{1}{m} \\
&> \sum_{m=1}^{k}\frac{1}{m} \\
&> \log(k+1).
\end{aligned}$$

The estimates can be found in [1], Section 19.1. We conclude that $n_k/\phi(n_k) \to \infty$ as claimed.

(c) Choose n_k as in part (b). Arguing as in part (a) we find that $\pi(an_k + b) < b + a\phi(n_k)$ for all $a \geq 0$ and $0 \leq b < n_k$. Hence

$$\frac{\pi(an_k+b)}{an_k+b} < \frac{b}{an_k+b} + \frac{a\phi(n_k)}{an_k+b} < \min(1, b/a) + \frac{\phi(n_k)}{n_k}.$$

Since can write any $n \in \mathbb{N}$ in the form $n = an_k + b$ with $b < n_k$. We conclude that

$$\limsup_n \frac{\pi(n)}{n} \leq \frac{\phi(n_k)}{n_k}.$$

From (b) we know that $\phi(n_k)/n_k$ can be arbitrarily small by choosing k large enough. Hence $\limsup_n \frac{\pi(n)}{n} = 0$, as required. □

References

[1] Frits Beukers, *Getaltheorie voor Beginners* Epsilson-uitgaven Utrecht.