Number theory: solutions to the sample exam paper 2010/11

1. Clearly, every integer n admits a unique representation of the form $n = k^2 l$, where l is square free. Thus,

$$\sum_{\substack{l \text{ square free,} \\ l \leq N}} \frac{1}{l} \sum_{k^2 \leq N} \frac{1}{k^2} \geq \sum_{n \leq N} \frac{1}{n}.$$

Since the latter sum tends to infinity as N tends to infinity, and

$$\sum_{k^2 \leq N} \frac{1}{k^2} \leq \sum_{k \geq 1} \frac{1}{k^2} \leq 1 + \sum_{k \geq 1} \frac{1}{k(k-1)} = 1 + \sum_{k \geq 1} (\frac{1}{(k-1)} - \frac{1}{k}) = 2,$$

we deduce that

$$\sum_{\substack{l \text{ square free,} \\ l \leq N}} \frac{1}{l}$$

tends to infinity as N tends to infinity. Also, this sum is clearly equal to

$$\prod_{p \text{ prime}} (1 + \frac{1}{p}),$$

so if there were only a finite number of primes, the sum would have to be finite too.

2. We have $r(x) = f(x) - (\frac{1}{2}x - \frac{1}{4})g(x) = \frac{11}{4}x^3 - \frac{3}{2}x^2 - 4x - \frac{5}{4}$, so

$$r_1(x) = g(x) - (\frac{8}{11}x + \frac{4}{121})r(x) = -\frac{368}{121}(x^2 - x - 1),$$

and

$$r_2(x) = r(x) + \frac{121}{368}(\frac{11}{4}x + \frac{5}{4})r_1(x) = 0.$$

This means that $\frac{121}{368}r_1(x)$ is the greatest common divisor. We have

$$\frac{121}{368}r_1(x) = \frac{121}{368}(g(x) - (\frac{8}{11}x + \frac{4}{121})(f(x) - (\frac{1}{2}x - \frac{1}{4})g(x))) =$$
$$= -(\frac{11}{46}x + \frac{1}{92})f(x) + (\frac{11}{92}x^2 - \frac{5}{92}x + \frac{15}{46})g(x).$$

3.(a) Let the decimal digits of n be a_0, a_1 etc., so that $n = a_0 + 10a_1 + 100a_2 + \ldots$. We have

$$n = a_0 + 10a_1 + 100a_2 + \ldots = (a_0 + a_1 + a_2 + \ldots) + (9a_1 + 99a_2 + 999a_3 + \ldots),$$

which instantly proves the statement we want to prove.

(b) In class, we proved that for the Euler function φ we have $\varphi(ab) = \varphi(a)\varphi(b)$ whenever a and b are coprime. Therefore, we have $\varphi(90) = \varphi(5)\varphi(9)\varphi(2) = 4 \cdot 6 \cdot 1 = 24$. By Euler's theorem, we have $a^{24} \equiv 1 \pmod{90}$ whenever $\gcd(a, 90) = 1$. This can be rewritten as $a^{23} \equiv a^{-1} \pmod{90}$.

(c) By (a),

$$n^{23} \equiv 9993565473468051560755525242941776485355563 \equiv$$
$$\equiv 9+9+9+3+5+6+5+4+7+3+4+6+8+0+5+1+5+6+0+$$
$$+7+5+5+5+2+5+2+4+2+9+4+1+7+7+6+4+8+5+3+5+5+6+3 \equiv$$
$$\equiv 205 \equiv 7 \pmod 9.$$

This means that n is coprime with 9; also, the remainder modulo 10 is the last decimal digit of a number, so $n^{23} \equiv 3 \pmod{10}$, which immediately shows that n is coprime with 10 Therefore, n is coprime with 90, so by (b), $n^{23} \equiv n^{-1} \pmod{90}$. This means that $n^{23} \equiv n^{-1} \pmod 9$ and $n^{23} \equiv n^{-1} \pmod{10}$. Summing up the above, we have the system of congruences

$$\begin{cases} n^{-1} \equiv 7 \pmod 9, \\ n^{-1} \equiv 3 \pmod{10}, \end{cases}$$

Since $10x - 9y = 1$ for $x = y = 1$, the Chinese remainder theorem implies that this system is equivalent to a single congruence $n^{-1} \equiv 10 \cdot 7 - 9 \cdot 3 = 43 \pmod{90}$.

Let us compute 43^{-1} modulo 90. The Euclidean algorithm for 43 and 90 proceeds as

$$\begin{aligned} 90 &= 2 \cdot 43 + 4, \\ 43 &= 10 \cdot 4 + 3, \\ 4 &= 3 + 1, \\ 3 &= 3 \cdot 1 + 0, \end{aligned}$$

so

$$\begin{aligned} 4 &= 90 - 2 \cdot 43, \\ 3 &= 43 - 10(90 - 2 \cdot 43) = 21 \cdot 43 - 10 \cdot 90, \\ 1 &= 11 \cdot 90 - 23 \cdot 43, \end{aligned}$$

so $n \equiv 43^{-1} \equiv (-23) \equiv 67 \pmod{90}$. We conclude that $n = 67$, otherwise n would be greater than 100, and n^{23} would have at least 46 decimal digits, which is not the case.

4. If for some integer n and an odd prime p we have $16n^2 - 2 \equiv 0 \pmod p$, we observe that $(4n)^2 \equiv 2 \pmod p$, so $\left(\frac{2}{p}\right) = 1$, and from class we know that it implies $p \equiv \pm 1 \pmod 8$. Also, since $16n^2 - 2 = 2(8n^2 - 1)$, we conclude that not all of odd prime divisors of $16n^2 - 2$ are congruent to 1 modulo 8, so there is at least one congruent to -1 modulo 8. From here, the proof proceeds as usual: if there are only finitely many primes of that form, put n equal to their product, and arrive to a contradiction.

5. If that inequality is satisfied, we have

$$\frac{1}{n^3} > \left|\sqrt{2} - \frac{m}{n}\right| = = \left|\frac{2 - \frac{m^2}{n^2}}{\sqrt{2} + \frac{m}{n}}\right| = \left|\frac{1}{n^2} \frac{2n^2 - m^2}{\sqrt{2} + \frac{m}{n}}\right| \geq \left|\frac{1}{\sqrt{2} + \frac{m}{n}}\right| \frac{1}{n^2}$$

because $|2n^2 - m^2| \geq 1$ (it is a nonzero integer), so

$$\frac{1}{n^3} > \left|\frac{1}{\sqrt{2} + \frac{m}{n}}\right| \frac{1}{n^2},$$

which implies

$$|\sqrt{2}+\frac{m}{n}|>n,$$

so

$$3+1>2\sqrt{2}+\frac{1}{n^3}>2\sqrt{2}+\left|-\sqrt{2}+\frac{m}{n}\right|\geq\left|2\sqrt{2}-\sqrt{2}+\frac{m}{n}\right|=\left|\sqrt{2}+\frac{m}{n}\right|>n,$$

which means $n<4$, so $n=1,2,3$, and clearly for each of these n there are only finitely many m that would work. For those n we have the inequalities $|\sqrt{2}-m|<1$, $|\sqrt{2}-\frac{m}{2}|<\frac{1}{8}$, and $|\sqrt{2}-\frac{m}{3}|<\frac{1}{27}$ respectively, which gives the solutions $n=1, m=1$; $n=1$, $m=2$; $n=2$, $m=3$. (For $n=3$ it is easy to that $m=4$ and $m=5$ do not work, and hence other choices of m would not work either.)

6. The case of odd p is obvious: there are two solutions ± 1, and if there is a solution for $(x-1)(x+1)=x^2-1\equiv 0 \pmod{p^k}$ different from ± 1, we observe that both $x-1$ and $x+1$ are divisible by p, so $2=(x+1)-(x-1)$ is divisible by p, a contradiction. For powers of two, the reasoning is as follows. Clearly, $x=2y+1$ for some y, because $x^2\equiv 1 \pmod{2^k}$ and is therefore odd. We have $x^2=4y^2+4y+1\equiv 1 \pmod{2^k}$, so $4y^2+4y\equiv 0 \pmod{2^k}$. For $k=1,2$ this is satisfied for any choice of y, so any odd x modulo 2^k would do, which explains the answer. For $k\geq 3$, that congruence is equivalent to $y(y+1)\equiv 0 \pmod{2^{k-2}}$, which clearly means $y\equiv 0 \pmod{2^{k-2}}$ or $y\equiv -1 \pmod{2^{k-2}}$. Finally, we have to pick those y which give different solutions for x modulo 2^k, which are $y=0$, $y=-1$, $y=2^{k-2}$, $y=2^{k-2}-1$, — altogether 4 solutions. Given that $43120=2^4\cdot 5\cdot 7^2\cdot 11$, and using the Chinese remainder theorem (choosing a solution modulo each prime power determines the solution uniquely), we instantly conclude that the number of solutions of $x^2\equiv 1 \pmod{43120}$ is $4\cdot 2\cdot 2\cdot 2=32$.