Math 322 (*Number Theory*). Final Exam, April 17, 2006.

1. Let $a_0, a_1, a_2, \ldots \in \mathbb{N}$, and let $\alpha := [a_0; a_1, a_2, \ldots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots +}}}$

For any $n \in \mathbb{N}$, we define the nth ***convergent*** and nth ***remainder***:

$$\frac{p_n}{q_n} := [a_0; a_1, a_2, \ldots, a_n] \qquad \text{and} \qquad r_n := [a_n; a_{n+1}, a_{n+2}, \ldots]$$

(Thus $p_0 = a_0$ and $q_0 = 1$, while $p_1 = a_0 a_1 + 1$ and $q_1 = a_1$.) Recall the recursion formulae:

$$\forall\ k \geq 2, \qquad p_k = a_k p_{k-1} + p_{k-2}, \tag{1}$$
$$\text{and} \qquad q_k = a_k q_{k-1} + q_{k-2}. \tag{2}$$

$(\frac{3}{100})$ (a) Verify case $k = 2$ of equations (1) and (2) by direct computation.

Solution: Note that

$$\frac{p_2}{q_2} := a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1 a_2 + 1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0(a_1 a_2 + 1) \ + \ a_2}{a_1 a_2 + 1}.$$

Thus,

$$p_2 = a_0(a_1 a_2 + 1) + a_2 = a_0 a_1 a_2 + a_2 + a_0 = a_2(a_0 a_1 + 1) + a_0 = a_2 p_1 + p_0,$$

while $q_2 = a_2 a_1 + 1 = a_2 q_1 + q_0$, as desired. □

$(\frac{5}{100})$ (b) Observe that $q_1 p_0 - p_1 q_0 = -1$. Prove that, for all $k \geq 2$, $\quad q_k p_{k-1} - p_k q_{k-1} = (-1)^k$.

Solution: (by induction) The base case $k = 1$ is just the above observation. Assume the theorem is true for $k - 1$. Then

$$\begin{aligned} q_k p_{k-1} - p_k q_{k-1} &\underset{(*)}{=} p_{k-1}(a_k q_{k-1} + q_{k-2}) - q_{k-1}(a_k p_{k-1} + p_{k-2}) \\ &= a_k p_{k-1} q_{k-1} + p_{k-1} q_{k-2} - a_k p_{k-1} q_{k-1} - q_{k-1} p_{k-2} \\ &= p_{k-1} q_{k-2} - q_{k-1} p_{k-2} \quad = \quad (-1)(q_{k-1} p_{k-2} - p_{k-1} q_{k-2}) \\ &\underset{(\dagger)}{=} (-1)(-1)^{k-1} \quad = \quad (-1)^k. \end{aligned}$$

Here $(*)$ is by substituting equations (1) and (2), and $(\dagger)$ is by induction hypothesis. □

$(\frac{2}{100})$ (c) Prove that, all $k \geq 2$, $\quad \dfrac{p_{k-1}}{q_{k-1}} - \dfrac{p_k}{q_k} = \dfrac{(-1)^k}{q_k q_{k-1}}$.

Solution: Divide both sides of the equation in part (b) by $q_k q_{k-1}$. □

$(\frac{5}{100})$ (d) Prove that, for any $k \geq 3$, $\quad \left|\alpha - \dfrac{p_k}{q_k}\right| + \left|\alpha - \dfrac{p_{k-1}}{q_{k-1}}\right| < \dfrac{1}{2q_k^2} + \dfrac{1}{2q_{k-1}^2}$

(**Hint:** *You may assume that either* $\dfrac{p_k}{q_k} < \alpha < \dfrac{p_{k-1}}{q_{k-1}}$ *or* $\dfrac{p_{k-1}}{q_{k-1}} < \alpha < \dfrac{p_k}{q_k}$.

You may also use the arithmetic/geometric mean inequality*:* $\sqrt{ab} \leq \frac{a+b}{2}$.)

Solution:

$$\left|\alpha-\frac{p_k}{q_k}\right|+\left|\alpha-\frac{p_{k-1}}{q_{k-1}}\right| \underset{(*)}{=} \left|\frac{p_k}{q_k}-\alpha+\alpha-\frac{p_{k-1}}{q_{k-1}}\right| = \left|\frac{p_k}{q_k}-\frac{p_{k-1}}{q_{k-1}}\right|$$
$$\underset{(\dagger)}{=} \left|\frac{(-1)^k}{q_k q_{k-1}}\right| = \frac{1}{q_k q_{k-1}} = \sqrt{\frac{1}{q_k^2 q_{k-1}^2}} \underset{(\ddagger)}{\leq} \frac{1}{q_k^2}+\frac{1}{q_{k-1}^2}.$$

Here $(*)$ is because α is between $\frac{p_k}{q_k}$ and $\frac{p_{k-1}}{q_{k-1}}$.

$(\dagger)$ is by part (c), and $(\ddagger)$ is the arithmetic/geometric mean inequality. □

$(\frac{5}{100})$ (e) Conclude, for any $k \geq 3$, at least one of the following two inequalities is true:

$$\text{either} \quad \left|\alpha-\frac{p_k}{q_k}\right| < \frac{1}{2q_k^2}, \qquad \text{or} \quad \left|\alpha-\frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2q_{k-1}^2}.$$

Solution: (by contradiction) Suppose neither was true. then $\left|\alpha-\frac{p_k}{q_k}\right| \geq \frac{1}{2q_k^2}$ and $\left|\alpha-\frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{2q_{k-1}^2}$. But then $\left|\alpha-\frac{p_k}{q_k}\right|+\left|\alpha-\frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{2q_k^2}+\frac{1}{2q_{k-1}^2}$, contradicting part (d). □

2. For any $n \in \mathbb{N}$, let $\mathbb{U}_n$ is multiplicative group of units mod n, and let $\mathcal{Q}_n \subset \mathbb{U}_n$ be the subgroup of quadratic residues, mod n. Recall the Multiplicative Chinese Remainder Theorem:

If n and m are relatively prime, then there is a group isomorphism $\Psi : \mathbb{U}_{nm} \longrightarrow \mathbb{U}_n \times \mathbb{U}_m$.

$(\frac{6}{100})$ (a) Show that $\Psi(\mathcal{Q}_{nm}) = \mathcal{Q}_n \times \mathcal{Q}_m$.

Solution: Let $u \in \mathbb{U}_{nm}$. If $\Psi(u) = (u_1, u_2) \in \mathbb{U}_n \times \mathbb{U}_m$, then $\Psi(u^2) = (u_1^2, u_2^2)$. Let $v \in \mathbb{U}_{nm}$, and let $\Psi(v) = (v_1, v_2) \in \mathbb{U}_n \times \mathbb{U}_m$. Thus,

$$\Big(u^2 = v\Big) \underset{(*)}{\Longleftrightarrow} \Big(\Psi(u^2) = \Psi(v)\Big) \Longleftrightarrow \Big((u_1^2, u_2^2) = (v_1, v_2)\Big) \Longleftrightarrow \Big(v_1 = u_1^2 \text{ and } v_2 = u_2^2\Big).$$

Here $(*)$ is because Ψ is injective. Thus,

$$\begin{aligned}\Big(v \in \mathcal{Q}_{nm}\Big) &\Longleftrightarrow \Big(\exists\, u \in \mathbb{U}_{nm} \text{ with } u^2 = v\Big)\\ &\Longleftrightarrow \Big(\exists\, u_1 \in \mathbb{U}_n \text{ and } u_2 \in \mathbb{U}_m \text{ with } u_1^2 = v_1 \text{ and } u_2^2 = v_2\Big)\\ &\Longleftrightarrow \Big(v_1 \in \mathcal{Q}_n \text{ and } v_2 \in \mathcal{Q}_m\Big) \Longleftrightarrow \Big(\Psi(v) \in \mathcal{Q}_n \times \mathcal{Q}_m\Big).\end{aligned}$$

□

$(\frac{4}{100})$ (b) Define $\omega : \mathbb{N} \longrightarrow \mathbb{N}$ by $\omega(n) = \#\mathcal{Q}_n$. Show that ω is a multiplicative function.

Solution: If $n, m \in \mathbb{N}$ are relatively prime, then

$$\omega(nm) = \#\mathcal{Q}_{nm} \underset{(*)}{=} \#\mathcal{Q}_n \times \#\mathcal{Q}_m = \omega(n)\omega(m),$$

where $(*)$ is by part (a). □

3. Suppose p and q are prime. Let $\lambda := \text{lcm}(p-1, q-1)$.

$(\frac{6}{100})$ (a) Show that, for any $u \in \mathbb{U}_{pq}$, $u^\lambda \underset{pq}{\equiv} 1$.

Solution: λ is a multiple of both $p-1$ and $q-1$. So, let $\lambda = n(p-1)$ and $\lambda = m(q-1)$. Then for any $u \in \mathbb{U}_p$, $u^\lambda = u^{n(p-1)} = (u^{p-1})^n \underset{p}{\equiv} 1^n = 1$. Here, "$\underset{p}{\equiv}$" is by Fermat's Little Theorem. Likewise, for any $v \in \mathbb{U}_q$, $v^\lambda = v^{m(q-1)} = (v^{q-1})^m \underset{q}{\equiv} 1^m = 1$.

Let $\Psi : \mathbb{U}_{pq} \longrightarrow \mathbb{U}_p \times \mathbb{U}_q$ be the isomorphism provided by the Chinese Remainder Theorem. If $w \in \mathbb{U}_{pq}$, and $\Psi(w) = (u, v) \in \mathbb{U}_p \times \mathbb{U}_q$, then $\Psi(w^\lambda) = \Psi(w)^\lambda = (u^\lambda, v^\lambda) = (1, 1) = \Psi(1)$. Thus, $w^\lambda \underset{pq}{\equiv} 1$ (because Ψ is bijective). □

$(\frac{4}{100})$ (b) Let $d, e \in \mathbb{U}_\lambda$ be such that $de \underset{\lambda}{\equiv} 1$. Define the 'modified' RSA encryption function $\epsilon : \mathbb{U}_{pq} \longrightarrow \mathbb{U}_{pq}$ and decryption function $\delta : \mathbb{U}_{pq} \longrightarrow \mathbb{U}_{pq}$ by

$$\delta(u) \quad := \quad u^d \qquad \text{and} \qquad \epsilon(u) \quad := \quad u^e, \qquad \text{for all } u \in \mathbb{U}_{pq}.$$

Show that $\delta \circ \epsilon(u) \underset{pq}{\equiv} u$ for all $u \in \mathbb{U}_{pq}$. (i.e. δ is a decryption function for ϵ)

Solution: If $de \underset{\lambda}{\equiv} 1$, then $de = m\lambda + 1$ for some $m \in \mathbb{Z}$. Thus, $\delta \circ \epsilon(u) = \delta(u^e) = u^{ed} = u^{m\lambda+1} = (u^\lambda)^m \cdot u \underset{(@)}{\equiv} 1 \cdot u = u$, where (@) is by part (a). □

$(\frac{5}{100})$ (c) Explain briefly why generating public/private key pairs (d, e) in this cryptosystem is generally more computationally efficient than it would be in than the 'standard' RSA cryptosystem. (**Hint:** *What is the complexity of computing an inverse, mod φ or mod λ?*)

Solution: In the RSA cryptosystem, the decryption exponent d is the inverse of the encryption exponent e in the group $\mathbb{U}_\varphi$, where $\varphi = \phi(pq) = (p-1)(q-1)$. In the above cryptosystem, d is the inverse e in the group $\mathbb{U}_\lambda$, where $\lambda = \text{lcm}(p-1, q-1)$. The size of φ and λ determines the computational complexity of computing these inverses. To be precise, we compute inverses (mod φ) by applying the Extended Euclidean Algorithm, which has complexity of order $\log(\varphi)$. Likewise, computing inverses (mod λ) has complexity $\log(\lambda)$.

However, $\lambda \leq \varphi$, because $\varphi = (p-1)(q-1)$ is a common multiple of $(p-1)$ and $(q-1)$, where λ is their *least* common multiple. Indeed, $\lambda = \frac{(p-1)(q-1)}{\gcd(p-1,q-1)}$, so $\log(\lambda) = \log(\varphi) - \log(g)$, where $g = \gcd(p-1, q-1)$. Thus, it is generally easier (and possibly much easier, if g is large) to compute inverses mod λ than mod φ. □

4. Let $n = pq$ where p and q are two large primes. The number n is public knowledge, but p and q are secret. The *Rabin cryptosystem* is based on the difficulty of computing square roots, mod n (and the relative ease of computing them, mod p and mod q. If $a \in \mathbb{U}_n$ be the 'plaintext', then $b := a^2$ is the cyphertext. To decrypt the cyphertext, we must compute a, given b.

$(\frac{5}{100})$ (a) Suppose you know p and q and suppose you can compute $a_1 \in \mathbb{U}_p$ and $a_2 \in \mathbb{U}_q$ such that $a_1^2 \underset{p}{\equiv} b$ and $a_2^2 \underset{q}{\equiv} b$. Explain how this information determines a.

Solution: The Chinese Remainder Theorem says there exists a unique $a \in \mathbb{U}_n$ such that $a \underset{p}{\equiv} a_1$ and $a \underset{q}{\equiv} a_2$. Then $a^2 \underset{p}{\equiv} a_1^2 \underset{p}{\equiv} b$ and $a^2 \underset{q}{\equiv} a_2^2 \underset{q}{\equiv} b$. But The Chinese Remainder Theorem says there exists a unique $x \in \mathbb{U}_n$ such that $x \underset{p}{\equiv} b$ and $x \underset{q}{\equiv} b$ —namely $x = b$. Thus, $a^2 \underset{n}{\equiv} b$, as desired. □

$(\frac{5}{100})$ (b) Suppose you *don't* know p and q, but you have a magic decryption machine such that, given any $b \in \mathbb{U}_n$, the machine produces a number $a \in \mathbb{U}_n$ such that $a^2 \underset{n}{\equiv} b$. We can use this machine to factor n into pq as follows:

- Pick a random integer a. Let $b := a^2$.
- Use the machine to obtain c such that $c^2 \underset{n}{\equiv} b$. (Thus, $c^2 \underset{p}{\equiv} b$ and $c^2 \underset{q}{\equiv} b$.) There are four possibilities (each with probability $\frac{1}{4}$):

$$\begin{array}{lllllll} (i) & c \underset{p}{\equiv} a & \text{and} & c \underset{q}{\equiv} a. & (ii) & c \underset{p}{\equiv} -a & \text{and} & c \underset{q}{\equiv} a. \\ (iii) & c \underset{p}{\equiv} a & \text{and} & c \underset{q}{\equiv} -a. & (iv) & c \underset{p}{\equiv} -a & \text{and} & c \underset{q}{\equiv} -a. \end{array}$$

- Let $g := \gcd(a + c, n)$.

Show that $g = p$ with probability $\frac{1}{4}$, and that $g = q$ with probability $\frac{1}{4}$.

Solution: In case (ii), $a + c \underset{p}{\equiv} a - a = 0$, whereas $a + c \underset{q}{\equiv} a + a = 2a \neq 0$. Thus, $p \mid (a + c)$ but $q \nmid (a + c)$; hence $\gcd(a + c, n) = \gcd(a + c, pq) = p$.

In case (iii), $a + c \underset{q}{\equiv} a - a = 0$, whereas $a + c \underset{p}{\equiv} a + a = 2a \neq 0$. Thus, $q \mid (a + c)$ but $p \nmid (a + c)$; hence $\gcd(a + c, pq) = q$.

(In case (i) $\gcd(a+c, n) = 1$, and in case (iv) $\gcd(a+c, n) = n$, which tells us nothing). □

$(\frac{5}{100})$ (c) Describe how the result in part (b) yields a 'Monte Carlo factoring algorithm' which has a very high probability of very rapidly factoring n. Explain why we interpret this result to mean that it is probably 'hard' to break the Rabin cryptosystem.

Solution: If we iterate the algorithm in part (b) k times, with k independent random choices of b, then the probability is $1 - \frac{1}{2^k} \approx 1$ that we will 'get lucky' at least once, and obtain either p or q.

Thus, a machine which breaks the Rabin cryptosystem is equivalent to a machine which can rapidly factor n into pq —in other words, it is a highly efficient, probabilistic factoring algorithm. It is believed that the Prime Factorisation problem is 'hard' (NP-hard, to be precise), so this means that breaking Rabin is also hard. □

5. Let $p \in \mathbb{P}$ be an odd prime. Recall that Fermat's Last Theorem Case I states:

> *There do not exist any coprime $a, b, c \in \mathbb{Z}$ such that $a^p + b^p + c^p = 0$ and yet a, b, c are all coprime to p.*

We will prove Germain's Theorem, which states: *Let p and q be odd primes. Suppose that*

(i) For any $x, y, z \in \mathbb{Z}$, if $x^p + y^p + z^p \underset{q}{\equiv} 0$ then $xyz \underset{q}{\equiv} 0$.

(ii) There exists no $r \in \mathbb{Z}$ such that $r^p \underset{q}{\equiv} p$.

Then Fermat's Last Theorem Case I holds for p.

Suppose (by contradiction) that $a^p + b^p + c^p = 0$ and yet $abc \underset{p}{\not\equiv} 0$. Observe that

$$-a^p = b^p + c^p = (b + c)(b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1}) \qquad (3)$$

$(\frac{5}{100})$ (a) Show that $(b+c)$ is coprime to $b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1}$.

Solution: (By contradiction) Let $m \in \mathbb{P}$ and suppose m divides $(b+c)$ and $(b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1})$. Then $b \underset{m}{\equiv} -c$, so that

$$b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1} \underset{m}{\equiv} b^{p-1} + b^{p-1} + \cdots + b^{p-1} + \quad = \quad pb^{p-1}.$$

Thus, $m \,\big|\, pb^{p-1}$, which means either $m \,\big|\, p$ or $m \,\big|\, b^{p-1}$ (By Lemma 2.1, because m is prime).

If $m \,\big|\, p$ then $m = p$ because both are prime. But then

$$p \quad = \quad m \quad \Big| \quad (b+c)(b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1}) \quad = \quad b^p + c^p \quad = \quad -a^p.$$

Thus, $p \,\big|\, a^p$, which means $p \,\big|\, a$, contradicting our assumption that a, b, c are coprime to p.

Thus, $m \,\big|\, b^{p-1}$. But then $m \,\big|\, b$ (because m is prime). Then m divides $c = (b+c) - b$. But then m also divides a^p, because equation (3) becomes

$$-a^p \quad = \quad b^p + c^p \underset{m}{\equiv} 0 + 0 \quad = \quad 0.$$

Thus, m divides a. At this point, $\gcd(a, b, c) \geq m$, contradicting the assumption that they are coprime. □

$(\frac{5}{100})$ (b) Show that there exist $r, s \in \mathbb{Z}$ such that the following equations hold:

$$(\mathbf{a}) \quad b + c \overset{(1)}{=} r^p \quad \text{and} \quad b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1} \overset{(2)}{=} u^p, \quad \text{so} \quad a \overset{(3)}{=} -ru.$$

Solution: Equation (3) implies that $(b+c)(b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1}) = -a^p$ is a perfect pth power. But these two factors are coprime by part (a). Thus, Lemma 2.4 says that $(b+c)$ and $(b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1})$ must each be perfect pth powers. That is, there exist r and u in $\mathbb{Z}$ making equations (a1) and (a2) true. Then equation (a3) then follows from equation (3). □

(Remark: *Notice that the roles of a, b, and c in this argument are completely symmetric. By applying the permutation $a \to b \to c \to a$, we deduce that there also exist $t, u, v, w \in \mathbb{Z}$ such that:*

$$\begin{array}{llllllllll} (\mathbf{b}) & c + a & \overset{(1)}{=} & s^p & \text{and} & c^{p-1} - c^{p-2}a + c^{p-3}a^2 - \cdots + a^{p-1} & \overset{(2)}{=} & v^p, & \text{so} \ b & \overset{(3)}{=} -sv. \\ (\mathbf{c}) & a + b & = & t^p & \text{and} & a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots + b^{p-1} & = & w^p, & \text{so} \ c & = -tw. \end{array}$$

If $a^p + b^p + c^p = 0$, then $a^p + b^p + c^p \underset{q}{\equiv} 0$. Thus, hypothesis (i) of Germain's theorem implies that one of a, b or c must be congruent to zero, mod q. We assume WOLOG that $c \underset{q}{\equiv} 0$. Thus,

$$u^p \underset{\text{(a2)}}{=\!=} b^{p-1} - b^{p-2}c + b^{p-3}c^2 - \cdots + c^{p-1} \underset{q}{\equiv} b^{p-1}. \tag{4}$$

Thus, $u \in \mathbb{U}_q$ because $u \perp q$ because $u^p = b^{p-1} \perp q$ because $b \perp q$.)

$(\frac{5}{100})$ (c) Deduce that one of r, s or t must be congruent to zero, mod q.

Solution: $r^p + s^p + (-t)^p \quad = \quad r^p + s^p - t^p \underset{(1)}{=\!=} (b+c) + (c+a) - (a+b) \quad = \quad 2c \underset{q}{\equiv} 0.$ here (1) is by column (1) in part (b). Thus, hypothesis (i) of Germain's theorem implies that one one of r, s or t must be congruent to zero, mod q. □

(Remark: *Through a simple argument we can show that $r \underset{q}{\not\equiv} 0$ and $s \underset{q}{\not\equiv} 0$. Thus, (c) implies that $t \underset{q}{\equiv} 0$.*)

$(\frac{5}{100})$ (d) Deduce that $w^p \underset{q}{\equiv} pb^{p-1}$.

Solution: If $t \underset{q}{\equiv} 0$, then $a+b \underset{(c1)}{=\!=} t \underset{q}{\equiv} 0$, so that $a \underset{q}{\equiv} -b$. Thus,

$$w^3 \underset{(c2)}{=\!=} a^{p-1}-a^{p-2}b+a^{p-3}b^2-\cdots+b^{p-1} \underset{q}{\equiv} b^{p-1}-b^{p-1}+b^{p-1}-\cdots+b^{p-1} = pb^{p-1}$$

□

$(\frac{5}{100})$ (e) Construct $r \in \mathbb{U}_q$ such that $r^p \underset{p}{\equiv} p$, contradicting hypothesis (ii) of Germain's Theorem. (Remark: *It follows that a, b, c cannot exist; this proves Germain's theorem.*)

Solution: Let i be the multiplicative inverse of u in $\mathbb{U}_q$ [which exists because $u \in \mathbb{U}_q$]. Let $r := wi$. Then

$$r^p = w^p i^p \underset{q}{\overset{(*)}{\equiv}} pb^{p-1}i^p \underset{q}{\overset{(\dagger)}{\equiv}} pu^p i^p = p(ui)^p \underset{q}{\overset{(\ddagger)}{\equiv}} p1^p = p.$$

Here, $(*)$ is by part (d), $(\dagger)$ is by equation (4), and $(\ddagger)$ is because $iu \underset{q}{\equiv} 1$ by definition of i. □

6. Let $\mathbb{S}_1 \subset \mathbb{N}$ be the set of squarefree numbers. (Recall: n is *square-free* if n is not divisible by any perfect square.) Let n be a 'random' integer. We will show that $\text{Prob}[n \in \mathbb{S}_1] = \dfrac{1}{\zeta(2)} \approx 0.607927101....$, where ζ is the Riemann zeta function.

For any $m \in \mathbb{N}$, let $\mathbb{S}_m := \{n \in \mathbb{N}\ ;\ \text{the largest square factor of } n \text{ is } m^2\}$.

(Thus, $\mathbb{S}_1$ is the set of squarefree numbers)

$(\frac{5}{100})$ (a) Show that $\mathbb{S}_m \subseteq m^2 \cdot \mathbb{S}_1$.

Solution: Let $n \in \mathbb{S}_m$. Then $m^2 \,\big|\, n$. Let $k := n/m^2$.

I claim $k \in \mathbb{S}_1$. To see this, suppose $\ell^2 \,\big|\, k$; then $\ell^2 m^2 \,\big|\, m^2 k = n$; hence $\ell = 1$ because m^2 is the largest square dividing n.

Thus, $n = m^2 k \in m^2 \mathbb{S}_1$. This holds for all $n \in \mathbb{S}_m$,so $\mathbb{S}_m \subseteq m^2 \cdot \mathbb{S}_1$. □

$(\frac{5}{100})$ (b) Show that $\mathbb{S}_m \supseteq m^2 \cdot \mathbb{S}_1$.

Solution: Let $k \in \mathbb{S}_1$, and let $n := m^2 k$. Then clearly $m^2 \,\big|\, n$. I claim $n \in \mathbb{S}_m$. To see this, suppose $n \in \mathbb{S}_\ell$ for some $\ell \geq m$. Then $\ell^2 \,\big|\, n$.

Claim 1: $m \,\big|\, \ell$.

Proof: Let $c := \text{lcm}(m, \ell)$. Then $c^2 = \text{lcm}(m^2, \ell^2)$, and c^2 divides n, because n is a common multiple of m^2 and ℓ^2. But this contradicts the maximality of ℓ, unless $c = \ell$, in which case $m \,\big|\, \ell$. ◇ Claim 1

Let $q = \ell/m$. Then $q^2 = \ell^2/m^2$, and $\ell^2 \,\big|\, n$, so $q^2 \,\big|\, (n/m^2) = k$. Thus, $q = 1$ because $k \in \mathbb{S}_1$. Thus, $\ell = m$.

Thus, $n = m^2 k \in \mathbb{S}_m$. This holds for all $k \in \mathbb{S}_1$,so $\mathbb{S}_m \supseteq m^2 \cdot \mathbb{S}_1$. □

$(\frac{5}{100})$ (c) For any subset $\mathbb{A} \subset \mathbb{N}$, let $\delta(\mathbb{A})$ be the probability[1] that a 'random' integer is in $\mathbb{A}$. It follows from (a) and (b) that $\mathbb{S}_m = m^2\mathbb{S}_1$, and thus, $\delta(\mathbb{S}_m) = \frac{1}{m^2}\delta(\mathbb{S}_1)$.

Conclude that $\dfrac{1}{\delta(\mathbb{S}_1)} = \sum_{m=1}^{\infty} \dfrac{1}{m^2}$, and thus, $\delta(\mathbb{S}_1) = \dfrac{1}{\zeta(2)}$.

Solution: Clearly, $\mathbb{N} = \bigsqcup_{m=1}^{\infty} \mathbb{S}_m$. Thus,

$$1 = \delta(\mathbb{N}) = \delta\left(\bigsqcup_{m=1}^{\infty} \mathbb{S}_m\right) = \sum_{m=1}^{\infty} \delta(\mathbb{S}_m) = \sum_{m=1}^{\infty} \frac{\delta(\mathbb{S}_1)}{m^2} = \delta(\mathbb{S}_1) \sum_{m=1}^{\infty} \frac{1}{m^2}$$

Thus, $\dfrac{1}{\delta(\mathbb{S}_1)} = \sum_{m=1}^{\infty} \dfrac{1}{m^2} =: \zeta(2)$. Thus, $\delta(\mathbb{S}_1) = \dfrac{1}{\zeta(2)}$, as desired. □

[1] Technically, $\delta(\mathbb{A}) := \lim_{N\to\infty} \dfrac{\#(\mathbb{A} \cap [1...N])}{N}$ is the *Cesàro density* of $\mathbb{A}$.