

## Solutions to the Number Theory Problems

**1:** Show that  $\lfloor (2 + \sqrt{3})^n \rfloor$  is odd for every positive integer  $n$ .

Solution: Notice that  $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n = \sum_{i=0}^n \binom{n}{i} 2^{n-i} \sqrt{3}^i + \sum_{i=0}^n (-1)^i \binom{n}{i} 2^{n-i} \sqrt{3}^i = 2 \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} 2^{n-2j} 3^j$ , which is an even number, and we have  $0 < (2 - \sqrt{3})^n < 1$ , so  $\lfloor (2 + \sqrt{3})^n \rfloor$  is odd.

**2:** Show that there is no non-constant polynomial  $f(x)$  with integral coefficients such that  $f(n)$  is prime for every positive integer  $n$ .

Solution: Suppose, for a contradiction, that  $f$  is such a polynomial. Let  $p = f(1)$ , which is prime. Note that when  $n = 1 \pmod p$ , we have  $f(n) = f(1) = 0 \pmod p$ , so  $p$  divides  $f(n)$ . Since  $f(n)$  is prime and  $p$  divides  $f(n)$ , we must have  $f(n) = p$ . Thus there are infinitely many values of  $n$  such that  $f(n) = p$ , and so the polynomial  $g(x) = f(x) - p$  has infinitely many roots. But then  $g(x) = 0$  for all  $x$  and so  $f(x) = p$  for all  $x$ .

**3:** Find all prime powers  $p^k$  with  $k > 1$  such that  $p^k = 2^n \pm 1$  for some integer  $n$ .

Solution: Suppose first that  $p^k = 2^n + 1$ . Then  $2^n = p^k - 1 = (p - 1)(p^{k-1} + p^{k-2} + \cdots + p + 1)$ , so  $(p - 1)$  and  $(p^{k-1} + \cdots + p + 1)$  are both powers of 2. Since  $p$  is odd and  $(p^{k-1} + \cdots + p + 1)$  is even,  $k$  must be even, say  $k = 2m$ . Then we have  $2^n = p^{2m} - 1 = (p^m - 1)(p^m + 1)$ , so  $(p^m - 1)$  and  $(p^m + 1)$  are powers of 2 that differ by 2, hence we must have  $p^m - 1 = 2$  and  $p^m + 1 = 4$ , and so  $p = 3$  and  $m = 1$ . Thus there is only one prime power  $p^k$  of the form  $2^k + 1$ , namely  $3^2 = 9$ .

Next we suppose that  $p^k = 2^n - 1$ . If  $n$  is even, say  $n = 2m$ , then we have  $p^k = 2^{2m} - 1 = (2^m + 1)(2^m - 1)$ , but then  $p \mid (2^m + 1)$  and  $p \mid (2^m - 1)$  so  $p = 1$ , which is not possible. Thus  $n$  must be odd, say  $n = 2m + 1$ . If  $k$  is even, say  $k = 2l$ , then  $p^{2l} = 2^{2m+1} - 1$ , but then since  $p$  is odd,  $p^2 = 1 \pmod 4$  so  $p^{2l} = 1 \pmod 4$ , so we would have  $2^{2m+1} = p^{2l} + 1 = 2 \pmod 4$ , so that  $m = 0$ , which is not possible. Thus  $k$  is odd, so we have  $p^k = 2^n - 1$  with  $k$  and  $n$  both odd. We have  $2^n = p^k + 1 = (p + 1)(p^{k-1} - p^{k-2} + \cdots \pm 1)$ , so  $(p + 1)$  is a power of 2, say  $p + 1 = 2^l$ . Then  $2^n = p^k + 1 = (2^l - 1)^k + 1 = ((2^l)^k - (2^l)^{k-1} + \cdots + (2^l) - 1) + 1 = (2^l)^k - (2^l)^{k-1} + \cdots + (2^l)$ , and this is an odd multiple of  $2^l$ . Since  $2^n$  is an odd multiple of  $2^l$  we must have  $2^n = 2^l$ . So we have  $2^n = p^k + 1 = (2^n - 1)^k + 1$ . This only happens when  $n = 1$  or when  $k = 1$ , neither of which is allowed. Thus there are no prime powers  $p^k$  of the form  $2^k - 1$ .

We remark that we never made use of the fact that  $p$  is prime.

**4:** Find all positive integers  $n$  such that  $n^4 + 4^n$  is prime.

Solution: When  $n = 1$ ,  $n^4 + 4^n = 5$ , which is prime. We claim that when  $n > 1$ ,  $n^4 + 4^n$  is not prime. When  $n$  is even,  $n^4 + 4^n$  is even and more than 2, so it is not prime. When  $n$  is odd, say  $n = 2k + 1$ , we make use of the factorization  $(x^4 + 4y^4) = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$  to get  $n^4 + 4^n = (2k + 1)^4 + 4^{2k+1} = (2k + 1)^4 + 4(2^k)^4 = ((2k + 1)^2 + 2(2k + 1)(2^k) + 2(2^k)^2)((2k + 1)^2 - 2(2k + 1)(2^k) + 2(2^k)^2)$ . Note that when  $k > 0$ , both factors are greater than 1.

5: Find all integral solutions to  $x^2 + y^2 + z^2 = x^2y^2$ .

Solution: Let  $(x_0, y_0, z_0)$  be a solution. Working modulo 4 we have the following: if all three of the numbers  $x_0, y_0$  and  $z_0$  are odd, then  $x_0^2 + y_0^2 + z_0^2 = 3 \pmod{4}$  but  $x_0^2y_0^2 = 1 \pmod{4}$ ; if two of the three numbers are odd then  $x_0^2 + y_0^2 + z_0^2 = 2 \pmod{4}$  but  $x_0^2y_0^2 = 1$  or  $0 \pmod{4}$ ; if one of the three numbers is odd then  $x_0^2 + y_0^2 + z_0^2 = 1 \pmod{4}$  while  $x_0^2y_0^2 = 0 \pmod{4}$ . Thus all three of the numbers  $x_0, y_0$  and  $z_0$  must be even, say  $x_0 = 2x_1, y_0 = 2y_1$  and  $z_0 = 2z_1$ . Note that we have  $x_1^2 + y_1^2 + z_1^2 = 4x_1^2y_1^2$ . Working modulo 4 we find that all three of the numbers  $x_1, y_1$  and  $z_1$  are even, say  $x_1 = 2x_2, y_1 = 2y_2$  and  $z_1 = 2z_2$ . Continuing in this way, we obtain a sequence of triples  $(x_k, y_k, z_k)$  with  $x_k^2 + y_k^2 + z_k^2 = 4^k x_k^2 y_k^2$  and with  $x_k = 2x_{k+1}, y_k = 2y_{k+1}$  and  $z_k = 2z_{k+1}$ . Since  $x_0 = 2x_1 = 2^2x_2 = \cdots = 2^k x_k = \cdots$  so that  $x_0$  is a multiple of  $2^k$  for every  $k$ , we must have  $x_0 = 0$ . Similarly,  $y_0 = z_0 = 0$ . Thus the only solution to the given equation is the zero solution.

6: (a) Prove Wilson's Theorem: for an integer  $n > 1$ ,  $n$  is prime  $\iff (n-1)! = -1 \pmod{n}$ .

Solution: If  $n = 4$  then we have  $(n-1)! = 3! = 6 = 2 \pmod{4}$ . If  $n = kl$  where  $1 < k < l < n$  then  $(n-1)! = 1 \cdot 2 \cdots k \cdots l \cdots (n-1)$  so  $n = kl \mid (n-1)!$  and we have  $(n-1)! = 0 \pmod{n}$ . If  $n = k^2$  with  $k > 2$  then we have  $1 < k < 2k < n$  so  $(n-1)! = 1 \cdot 2 \cdots k \cdots (2k) \cdots n$  and so  $n = k^2 \mid (n-1)!$  and hence  $(n-1)! = 0 \pmod{n}$ . Thus when  $n$  is composite, if  $n = 4$  then  $(n-1)! = 2 \pmod{n}$ , and if  $n > 4$  then  $(n-1)! = 0 \pmod{n}$ .

Suppose that  $n = p$  is prime. When  $p = 2$  we have  $(p-1)! = 1 = -1 \pmod{p}$ , so suppose  $p$  is odd. Let  $f(x) = x^{p-1} - 1$ . By Fermat's Little Theorem,  $f(x) = 0$  in  $\mathbf{Z}_p$  for every  $x \in \mathbf{Z}_p$ , and so  $f(x)$  factors in  $\mathbf{Z}_p[x]$  as  $f(x) = (x-1)(x-2)\cdots(x-(p-1))$ . Put in  $x = 0$  to get  $-1 = (-1)^{p-1}(p-1)! \in \mathbf{Z}_p$ . Since  $p$  is odd this gives  $(p-1)! = -1 \in \mathbf{Z}_p$ .

(b) Show that for a positive integer  $n > 1$ ,  $\left\lfloor \frac{(n-1)!+1}{n} \right\rfloor - \left\lfloor \frac{(n-1)!}{n} \right\rfloor = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{if } n \text{ is composite} \end{cases}$

Solution: Suppose that  $n$  is prime. Then we have  $(n-1)! = -1 \pmod{n}$ , say  $(n-1)! = -1 + kn$ . Then  $\left\lfloor \frac{(n-1)!+1}{n} \right\rfloor - \left\lfloor \frac{(n-1)!}{n} \right\rfloor = \left\lfloor k - \left[k - \frac{1}{n}\right] \right\rfloor = \left\lfloor k - (k-1) \right\rfloor = 1$ . Now suppose that  $n = 4$ . Then  $\left\lfloor \frac{(n-1)!+1}{n} \right\rfloor - \left\lfloor \frac{(n-1)!}{n} \right\rfloor = \left\lfloor \frac{7}{4} - \left[\frac{3}{2}\right] \right\rfloor = \left\lfloor \frac{7}{4} - 1 \right\rfloor = 0$ . Finally, suppose that  $n$  is composite with  $n > 4$ . Then  $(n-1)! = 0 \pmod{n}$ , say  $(n-1)! = kn$ . Then  $\left\lfloor \frac{(n-1)!+1}{n} \right\rfloor - \left\lfloor \frac{(n-1)!}{n} \right\rfloor = \left\lfloor k + \frac{1}{n} - [k] \right\rfloor = \left\lfloor k + \frac{1}{n} - k \right\rfloor = \left\lfloor \frac{1}{n} \right\rfloor = 0$ .

7: (a) Show that there are infinitely many primes of the form  $4n+3$  where  $n$  is an integer.

Solution: Let  $p_1, p_2, \dots, p_k$  be any list of primes of the form  $4n+3$ . Consider the number  $m = 4p_1p_2\cdots p_k - 1$ . Since  $m$  is odd, its prime factors are odd, and every odd number is equal to 1 or 3 mod 4. It is not possible that every prime factor of  $m$  is equal to 1 mod 4, since  $m = 3 \pmod{4}$ . Thus  $m$  must have some prime factor, say  $p$ , which is equal to 3 mod 4. Note that  $p$  is not equal to any of the primes  $p_1, p_2, \dots, p_k$  since they are not factors of  $m$ . Thus given any  $k$  primes of the form  $4n+3$ , there exists another such prime.

(b) Show that there are infinitely many primes of the form  $4n+1$  where  $n$  is an integer.

Solution: We claim that for any integer  $a$ , the number  $a^2 + 1$  has no prime factors of the form  $4n+3$ . To prove this, let  $p$  be any odd prime factor of  $a^2 + 1$ . Then  $a^2 = -1 \pmod{p}$ . Raise both sides to the power of  $(p-1)/2$  to get  $a^{p-1} = (-1)^{(p-1)/2}$ . Since  $a^2 = -1 \pmod{p}$ ,  $p$  is not a factor of  $a$ , so by Fermat's Little Theorem  $a^{p-1} = 1 \pmod{p}$ , and so we have  $1 = (-1)^{(p-1)/2} \pmod{p}$ . Thus  $(p-1)/2$  must be even and so  $p$  must be of the form  $4n+1$ . This proves the claim.

Now let  $p_1, p_2, \dots, p_k$  be any primes of the form  $4n+1$ . Consider the number  $m = (2p_1p_2\cdots p_k)^2 + 1$ . Since  $m$  is odd it has an odd prime factor, say  $p$ , and since  $m$  is of the form  $a^2 + 1$ , the prime  $p$  must be of the form  $4n+1$ . Note that  $p$  is not equal to any of the primes  $p_1, p_2, \dots, p_k$  since they are not factors of  $m$ .

**8:** For a positive integer  $n$ , let  $\tau(n)$  denote the number of positive divisors of  $n$  and let  $\sigma(n)$  denote the sum of the positive divisors of  $n$ .

(a) Show that if  $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$  is the prime factorization of  $n$  then  $\tau(n) = \prod_{i=1}^m (k_i + 1)$  and  $\sigma(n) = \prod_{i=1}^m \frac{p_i^{k_i+1} - 1}{p_i - 1}$

Solution: The positive factors of  $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$  are of the form  $p_1^{j_1} p_2^{j_2} \cdots p_m^{j_m}$  with  $0 \leq j_i \leq k_i$  for all  $i$ . Since there are  $k_i + 1$  choices for the exponent  $j_i$ , the total number of factors is  $\tau(n) = \prod_{i=1}^m (k_i + 1)$ .

The factors of  $p^k$  are  $1, p, p^2, \dots, p^k$ , so we have  $\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}$ . Thus to show that the given formula for  $\sigma(n)$  is correct, it suffices to show that  $\sigma(rs) = \sigma(r)\sigma(s)$  whenever  $\gcd(r, s) = 1$ . When  $\gcd(r, s) = 1$ , the divisors  $d|rs$  are of the form  $d = ab$  where  $a|r$  and  $b|s$ , so we have  $\sigma(rs) = \sum_{d|rs} d = \sum_{a|r} \sum_{b|s} ab = \left( \sum_{a|r} a \right) \left( \sum_{b|s} b \right) = \sigma(r)\sigma(s)$ , as desired.

(b) For which positive integers  $n$  is  $\tau(n)$  odd?

Solution:  $\tau(n)$  is odd when all primes have an even exponent in the prime factorization of  $n$ , that is when  $n$  is a square.

(c) For which positive integers  $n$  is  $\sigma(n)$  odd?

Solution: Note that  $\sigma(2^k) = (1 + 2 + 4 + \cdots + 2^k)$  is odd for all values of  $k \geq 1$ , and note that for an odd prime  $p$ ,  $\sigma(p^k) = (1 + p + p^2 + \cdots + p^k)$  is odd when  $k$  is even, so  $\sigma(n)$  is odd when all odd primes have an even exponent in the prime factorization of  $n$ , that is when  $n$  is either a square or twice a square.

(d) For which positive integers  $n$  do we have  $\phi(n) + \sigma(n) = 2n$ ?

Solution: We claim that for  $n > 1$ ,  $\phi(n) + \sigma(n) = 2n$  when  $n$  is prime and  $\phi(n) + \sigma(n) > 2n$  when  $n$  is composite. When  $p$  is prime we have  $\phi(p) + \sigma(p) = (p - 1) + (1 + p) = 2p$ . When  $p$  is prime and  $k \geq 2$  we have  $\phi(p^k) + \sigma(p^k) = (p^k - p^{k-1}) + (1 + p + \cdots + p^{k-1} + p^k) = 2p^k + (1 + p + \cdots + p^{k-2}) > 2p^k$ . Finally, suppose that  $r > 1$  and  $s > 1$  are coprime with  $\phi(r) + \sigma(r) \geq 2r$  and  $\phi(s) + \sigma(s) \geq 2s$ . We need to show that  $\phi(rs) + \sigma(rs) > 2rs$ . Let  $\epsilon(r) = r - \phi(r)$  and  $\epsilon(s) = s - \phi(s)$ . Note that  $\epsilon(r) > 0$  and  $\epsilon(s) > 0$ . Also, since  $\phi(r) + \sigma(r) \geq 2r$  we have  $r - \epsilon(r) + \sigma(r) \geq 2r$  so  $\sigma(r) \geq r + \epsilon(r)$ . Similarly  $\sigma(s) \geq s + \epsilon(s)$ , and so  $\phi(rs) + \sigma(rs) = \phi(r)\phi(s) + \sigma(r)\sigma(s) \geq (r - \epsilon(r))(s - \epsilon(s)) + (r + \epsilon(r))(s + \epsilon(s)) = 2rs + 2\epsilon(r)\epsilon(s) > 2rs$ .

**9:** (a) Show that if  $2^k + 1$  is prime then  $k$  must be a power of 2.

Solution: We remark that when  $r$  is odd,  $x = -1$  is a root of  $x^r + 1$ , so  $x + 1$  is a factor of  $x^r + 1$ . Suppose that  $k$  is not a power of 2. Then we can write  $k = 2^n r$  for some  $n \geq 0$  and some odd number  $r > 1$ , and then we have  $2^k + 1 = 2^{2^n r} + 1$ . By the above remark,  $2^{2^n} + 1$  is a factor of  $2^{2^n r} + 1 = 2^k + 1$ , so  $2^k + 1$  is not prime.

(b) Let  $F_k = 2^{2^k} + 1$ . Show that if  $k \neq l$  then  $F_k$  and  $F_l$  are coprime.

Solution: We remark that  $x = -1$  is a root of  $x^{2^n} - 1$  and so  $x + 1$  is a factor of  $x^{2^n} - 1$ . Let  $k < l$ . We claim that  $F_k | (F_l - 2)$ . Write  $n = l - k$ . Then  $F_l - 2 = 2^{2^l} - 1 = 2^{2^{k+n}} - 1 = \left(2^{2^k}\right)^{2^n} - 1$ . By the above remark,  $2^{2^k} + 1$  is a factor of  $\left(2^{2^k}\right)^{2^n} - 1$ , that is  $F_k | (F_l - 2)$ , as claimed. Since  $F_k | (F_l - 2)$  and  $F_k$  and  $F_l$  are odd, it follows that  $F_k$  and  $F_l$  are coprime.

**10:** (a) Let  $a > 1$  and  $k > 1$  be integers. Show that if  $a^k - 1$  is prime then  $a = 2$  and  $k$  is prime.

Solution: Suppose that  $a > 2$ . Then  $a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$ , and  $(a - 1) > 1$  and  $(a^{k-2} + a^{k-1} + \cdots + a + 1) > 1$ , so  $a^k - 1$  is not prime. Thus if  $a^k - 1$  is prime then we must have  $a = 2$ . Now suppose that  $a = 2$  and that  $k = lm$  with  $1 < l$  and  $1 < m$ . Then  $a^k - 1 = 2^{lm} - 1 = (2^l)^m - 1 = (2^m - 1)((2^m)^{l-1} + \cdots + (2^m) + 1)$ , so  $2^m - 1$  is a factor of  $2^{lm} - 1$ . Since  $1 < 2^m - 1 < 2^{lm} - 1$  it follows that  $2^{lm} - 1$  is not prime.

(b) Let  $M_k = 2^k - 1$ . Show that if  $k$  and  $l$  are coprime then so are  $M_k$  and  $M_l$ .

Solution: Suppose that  $M_k$  and  $M_l$  are not coprime. Let  $d = \gcd(M_k, M_l)$ . Note that  $d$  is odd (since  $M_k$  and  $M_l$  are odd), so 2 is an invertible element in  $\mathbf{Z}_d$ . Let  $n$  be the order of 2 in  $\mathbf{Z}_d$  (so  $n$  is the smallest positive integer such that  $2^n = 1$  in  $\mathbf{Z}_d$ ). Since  $d | M_k = 2^k - 1$  we have  $2^k = 1 \in \mathbf{Z}_d$  and so  $n | k$ . Similarly  $n | l$  and so  $\gcd(k, l) \geq n > 1$ .

(c) Show that if  $p$  is prime and  $q$  is a prime divisor of  $M_p = 2^p - 1$ , then  $q = 1 \pmod{2p}$ .

Solution: Let  $q$  be a prime divisor of  $M_p$ . By Fermat's Little Theorem we have  $2^{q-1} = 1 \pmod{q}$  and so  $q | (2^{q-1} - 1) = M_{q-1}$ . Since  $q | M_{q-1}$  and  $q | M_p$ , we have  $\gcd(M_{q-1}, M_p) \neq 1$ , so by part (b)  $\gcd(q - 1, p) \neq 1$ . Since  $p$  is prime, this implies that  $p | (q - 1)$  so  $q = 1 \pmod{p}$ . Since  $q$  and  $p$  are both odd,  $q = 1 \pmod{2p}$ .

(d) List the 6 smallest prime numbers of the form  $M_p = 2^p - 1$  with  $p$  prime.

Solution: We have  $M_2 = 3$ ,  $M_3 = 7$ ,  $M_5 = 31$ ,  $M_7 = 127$ ,  $M_{11} = 2047$ ,  $M_{13} = 8191$  and  $M_{17} = 131071$ . The first 4 of these, 3, 7, 31 and 127 are easily seen to be prime. If  $q$  is a prime factor of  $M_{11}$  then by part (c) we have  $q = 1 \pmod{22}$ , that is  $q = 1, 23, 45, \dots$ . We try  $q = 23$  and find that  $M_{11} = 23 \cdot 89$ , so  $M_{11}$  is not prime. If  $q$  is a prime factor of  $M_{13}$  then  $q = 1 \pmod{26}$ . The only such primes with  $q \leq \sqrt{M_{13}}$  are  $q = 53$  and  $79$ . We test 53 and 79 and find they are not factors of  $M_{13}$ , so  $M_{13}$  is prime. Finally, if  $q$  is a prime factor of  $M_{17}$  then by part (c) we have  $q = 1 \pmod{34}$ , and the only primes  $q$  with  $q = 1 \pmod{34}$  and  $q \leq \sqrt{M_{17}}$  are  $q = 103, 137, 239$  and  $307$ . We try each of these and find they are not factors of  $M_{17}$ .

**11:** Show that every rational number  $p/q$ , where  $p$  and  $q$  are integers with  $0 < p < q$ , can be represented as a sum of distinct fractions of the form  $1/n$ , where  $n$  is a positive integer.

Solution: Given the rational number  $\frac{p}{q}$  with  $0 < p < q$ , we choose that smallest positive integer  $n_1$  with  $\frac{1}{n_1} \leq \frac{p}{q}$ , then if  $\frac{1}{n_1} \neq \frac{p}{q}$  we choose the smallest positive integer  $n_2$  such that  $\frac{1}{n_1} + \frac{1}{n_2} \leq \frac{p}{q}$ , then if  $\frac{1}{n_1} + \frac{1}{n_2} \neq \frac{p}{q}$  we choose the smallest positive integer  $n_3$  such that  $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \leq \frac{p}{q}$ , and so on. Note that we have  $1 < n_1 < n_2 < n_3 < \dots$  since if we had  $n_{k+1} \leq n_k$  then we would have  $\frac{p}{q} \geq \frac{1}{n_1} + \cdots + \frac{1}{n_{k-1}} + \frac{1}{n_k} + \frac{1}{n_{k+1}} \geq \frac{1}{n_1} + \cdots + \frac{1}{n_{k-1}} + \frac{2}{n_k} \geq \frac{1}{n_1} + \cdots + \frac{1}{n_{k-1}} + \frac{1}{n_{k-1}} + \frac{1}{n_{k-1}}$  contradicting our choice of  $n_k$ . Also note that by our choice of  $n_1$  we have  $\frac{1}{n_1} \leq \frac{p}{q} < \frac{1}{n_1 - 1}$  so  $n_1 - 1 < \frac{q}{p}$  and so  $pn_1 - p < q$  and hence  $pn_1 - q < p$ , and so the numerator of  $\frac{p}{q} - \frac{1}{n_1} = \frac{pn_1 - q}{qn_1}$  is smaller than the numerator of  $\frac{p}{q}$ . Similarly, we see that the numerators of the fractions  $\frac{p}{q} - \frac{1}{n_1} - \cdots - \frac{1}{n_k}$  decrease with each value of  $k$ . Eventually, the numerator becomes zero, and we obtain  $\frac{p}{q} = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$ .

**12:** Let  $\alpha$  and  $\beta$  be positive irrational numbers such that  $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ . For  $n \geq 1$  let  $a_n = \lfloor n\alpha \rfloor$  and let  $b_n = \lfloor n\beta \rfloor$ . Show that the two sequences  $\{a_n\}$  and  $\{b_n\}$  are disjoint and that every positive integer occurs as a term in one of the two sequences.

Solution: Suppose, for a contradiction, that  $\{a_n\}$  and  $\{b_n\}$  are not disjoint, say  $\lfloor n\alpha \rfloor = \lfloor m\beta \rfloor = k$ . Since  $\alpha$  and  $\beta$  are irrational, we have  $k < n\alpha < k + 1$  and  $k < m\beta < k + 1$ . Since ( $k < n\alpha$  and  $k < m\beta$ ) we have ( $\frac{n}{k} > \frac{1}{\alpha}$  and  $\frac{m}{k} > \frac{1}{\beta}$ ) and so  $\frac{n+m}{k} > \frac{1}{\alpha} + \frac{1}{\beta} = 1$ , and hence  $n + m > k$ . Similarly, since ( $n\alpha < k + 1$  and  $m\beta < k + 1$ ), we have  $n + m < k + 1$ . This gives the desired contradiction, since we cannot have  $k < n + m < k + 1$ , so the sequences  $\{a_n\}$  and  $\{b_n\}$  are disjoint.

Note that since  $\frac{1}{\alpha} + \frac{1}{\beta} = 1$  we have  $\frac{1}{\alpha} < 1$  so  $\alpha > 1$ , and so  $\lfloor n\alpha \rfloor < \lfloor (n+1)\alpha \rfloor$ . Thus the elements of  $\{a_n\}$  are distinct. Also note that since  $\lfloor \frac{k}{\alpha} \rfloor < \frac{k}{\alpha}$ , we have  $\lfloor \frac{k}{\alpha} \rfloor \alpha < k$ , and since  $\lfloor \frac{k}{\alpha} \rfloor > \frac{k}{\alpha} - 1$  we have  $\lfloor \frac{k}{\alpha} \rfloor \alpha > k - \alpha$  so  $(\lfloor \frac{k}{\alpha} \rfloor + 1)\alpha > k$ , and so the number of elements in the sequence  $\{a_n\}$  which are less than  $k$  is equal to  $\lfloor \frac{k}{\alpha} \rfloor$ . Similarly, the number of elements in the sequence  $\{b_n\}$  which are less than  $k$  is equal to  $\lfloor \frac{k}{\beta} \rfloor$ . Thus in order to show that every positive integer occurs as a term in one of the two sequences, it suffices to show that  $\lfloor \frac{k}{\alpha} \rfloor + \lfloor \frac{k}{\beta} \rfloor = k - 1$  for every positive integer  $k$ .

Since  $\frac{k}{\alpha} - 1 < \lfloor \frac{k}{\alpha} \rfloor < \frac{k}{\alpha}$  and  $\frac{k}{\beta} - 1 < \lfloor \frac{k}{\beta} \rfloor < \frac{k}{\beta}$ , we have  $k - 2 = \frac{k}{\alpha} + \frac{k}{\beta} - 2 < \lfloor \frac{k}{\alpha} \rfloor + \lfloor \frac{k}{\beta} \rfloor < \frac{k}{\alpha} + \frac{k}{\beta} = k$ , and so  $\lfloor \frac{k}{\alpha} \rfloor + \lfloor \frac{k}{\beta} \rfloor = k - 1$ , as required.