

1 Solutions to selected problems

- (2) When m is odd we have the polynomial factorisation

$$x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \dots - x + 1).$$

Suppose that n is not a power of 2, i.e. n contains an odd divisor $m > 1$. Suppose $n = m \cdot k$. Substitute $x = 2^k$ in the above identity, then

$$2^n + 1 = 2^{mk} + 1 = (2^k + 1)(2^{k(m-1)} - 2^{k(m-2)} + \dots - 2^k + 1).$$

So $2^k + 1$ is a divisor of $2^n + 1$. It remains to point out that it is a non-trivial divisor, i.e. $1 < 2^k + 1 < 2^n + 1$. So $2^n + 1$ is not prime, a contradiction. Therefore n cannot contain odd divisors > 1 .

- (3) When m is odd we have the polynomial factorisation

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \dots + x + 1).$$

Suppose that n is not a prime i.e. $n = m \cdot k$ for some integers $k, m > 1$. Substitute $x = 2^k$ in the above identity, then

$$2^n - 1 = 2^{mk} - 1 = (2^k - 1)(2^{k(m-1)} + 2^{k(m-2)} + \dots + 2^k + 1).$$

So $2^k - 1$ is a divisor of $2^n - 1$. It remains to point out that it is a non-trivial divisor, i.e. $1 < 2^k - 1 < 2^n - 1$. So $2^n - 1$ is not prime, a contradiction. Therefore n cannot be composite.

- (6) Suppose that $p + 2$ is composite for only finitely many primes p . Then there is a number P_0 such that p prime and $p > P_0$ implies $p + 2$ prime. Choose a prime $p > P_0$. Then, consequently, all odd numbers larger than p are prime. This is clearly impossible since, for example, all powers of 3 are composite. We get a contradiction.

- (8) Since n is odd we can write $n = 2m + 1$. Hence

$$n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 8 \binom{m+1}{2} + 1.$$

So we see that n^2 is 1 modulo 8.

- (10) For a),b) we refer to the course notes. Let $\eta = (1 + \sqrt{5})/2$, the golden ratio. Note that $\eta^2 = \eta + 1$.

Part c) When $n = k$ we must prove that $r_k \geq 1$ which is clearly true, since r_k is the last non-zero remainder. When $n = k - 1$ we must show that $r_{k-1} \geq \eta$ which is true as well, since $r_{k-1} \geq 2$. Now we apply induction using

$$\begin{aligned} r_{n-2} &= q_{n-1}r_{n-1} + r_n \\ &\geq r_{n-1} + r_n \\ &\geq \eta^{k-n+1} + \eta^{k-n} = \eta^{k-n}(\eta + 1) \\ &= \eta^{k-n}\eta^2 = \eta^{k-n+2} \end{aligned}$$

Part d) We have $a = r_{-1}$ and $r_{-1} \geq \eta^{k+1}$. Hence $\eta^{k+1} \leq a$, from which our desired inequality follows.

- (12) We give a hint. Suppose $n > m$ and suppose $n = mq + r$ with $0 \leq r < m$. Notice that we have the polynomial identity

$$(x^n - 1) = (x^m - 1)(x^{n-m} + x^{n-2m} + \cdots + x^{n-qm}) + x^r - 1.$$

By application of the euclidean algorithm to $a^n - 1$ and $a^m - 1$ we see that the exponents are precisely the remainders of the euclidean algorithm applied to n, m .

- (13) Let k be the number of zeros. In other words, k is the highest power such that 10^k divides $123!$. Since there are more factors 2 than 5 in $123!$, it suffices to count the number of factors 5. Between 1 and 123 there are 24 five-tuples and 4 twentyfive-tuples (twentyfive-tuples are also counted as five-tuples). There are no hundredtwentyfive-tuples or higher between 1 and 123. In total this gives us $24+4$ factors 5. Hence $k = 28$.
- (14a) Consider the numbers 1 to n . Among these numbers there are $[n/p]$ p -tuples, $[n/p^2]$ p^2 -tuples, $[n/p^3]$ p^3 -tuples, etc. Here we count p^k -tuples also as p^{k-1} -tuples. The total number of factors p in $n!$ therefore equals

$$\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \cdots$$

- (16) A perfect number n is characterised by $\sigma(n) = 2n$. In other words, $\sum_{d|n} d = 2n$ divide on both sides by n to obtain

$$\sum_{d|n} \frac{d}{n} = 2.$$

Notice that as d runs over the divisors of n , the number d/n runs over all inverses of the divisors of n . Hence

$$\sum_{d|n} \frac{1}{d} = 2.$$

- (18) All convolution products are convolution products of multiplicative functions. Hence the convolution products are also multiplicative. To describe the products it suffices to describe their values in the prime powers. Here are the results,

- (a) $(I_k * I_k)(n) = \sigma_0(n)n^k$
- (b) $\mu * I_1 = \phi$
- (c) $(\mu * \mu)(p^k) = -2$ als $k = 1$, 1 als $k = 2$, 0 als $k > 2$
- (d) $(\mu * 2^\omega)(n) = |\mu(n)|$
- (e) $(2^\omega * 2^\omega)(p^k) = 4k$
- (f) $(\mu * \phi)(p^k) = p^k - 2p^{k-1} + p^{k-2}$ if $k \geq 2$, $p - 2$ if $k = 1$.

- (22) We shall prove something more general. Let $f(n)$ be any arithmetic function with $f(1) \neq 0$. Then there exists an arithmetic function g such that $f * g = e$. In other words, we must determine numbers $g(1), g(2), g(3), \dots$ such that $f(1)g(1) = 1$ and for all $n > 1$,

$$\sum_{d|n} f(d)g(n/d) = 0$$

Hence $g(1) = 1/f(1)$ and for $n = 2, 3, 4, \dots$,

$$f(1)g(n) = - \sum_{d|n, d < n} g(d)f(n/d).$$

Note that the latter relation allows us to determine $g(2), g(3), g(4), \dots$ recursively.

To complete our exercise, we must show that if f is multiplicative, then so is g . Let m, n be relatively prime. Consider the relations

- (23) There is an error in the formulation of the problem, σ_1 should be σ_0 .

Notice that both lefthand side and righthand side are multiplicative functions. Thus it suffices to show equality when n is a prime power p^k . Note that

$$\sum_{d|p^k} \sigma_0(d)^3 = \sum_{l=0}^k \sigma_0(p^l)^3 = \sum_{l=0}^k (l+1)^3.$$

Also note that

$$\left(\sum_{d|p^k} \sigma_0(d) \right)^2 = \left(\sum_{l=0}^k \sigma_0(p^l) \right)^2 = \left(\sum_{l=0}^k (l+1) \right)^2.$$

The two results are equal because we have the famous identity

$$1^3 + 2^3 + \dots + (k+1)^3 = (1 + 2 + \dots + (k+1))^2$$

for all positive integers k .

- (24) Suppose that $n = ab$ with $1 < a < b < n$. Then the product $(n-1)!$ contains both factors a and b . Hence ab divides $(n-1)!$. Suppose n is composite and suppose it cannot be written as a product of two distinct numbers $a, b < n$. Then n must be the square of a prime p , i.e. $n = p^2$. We have assumed $n > 4$, so $p > 2$. But in that case the product $(n-1)!$ contains the factors p and $2p$. So p^2 divides $(n-1)!$.
- (26) Note that a number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. The alternating sum of the digits of a palindromic number of even length is zero.
- (27) Answers: 3 (mod 7), 13 (mod 71), 83 (mod 183).
- (29) Answers:
- a) $x \equiv 1307 \pmod{2100}$

b) $y \equiv 675 \pmod{1540}$

c) $z \equiv 193 \pmod{420}$

- (31) Instead of a million consecutive numbers we can more generally ask for n consecutive numbers, where n is any integer. We choose n distinct primes p_1, p_2, \dots, p_n and solve the simultaneous system of congruences

$$x + 1 \equiv 0 \pmod{p_1^2} \quad x + 2 \equiv 0 \pmod{p_2^2} \quad \dots \quad x + n \equiv 0 \pmod{p_n^2}.$$

Since the numbers p_i^2 are pairwise relatively prime, the Chinese remainder theorem shows the existence of a solution $x \in \mathbb{N}$. Hence $x + 1, x + 2, \dots, x + n$ is a sequence of n consecutive numbers all divisible by a square > 1 .

- (32) Notice that by the chinese remainder theorem,

$$a^2 \equiv a \pmod{10^k} \iff a^2 \equiv a \pmod{2^k}, \quad a^2 \equiv a \pmod{5^k}.$$

Suppose we want to solve $a^2 \equiv a \pmod{p^k}$ for any prime p . Observe that the equation is equivalent to $p^k | a^2 - a$, hence $p^k | a(a - 1)$. Since a and $a - 1$ are relatively prime, we have either $p^k | a$ or $p^k | a - 1$. In other words, $a \equiv 0 \pmod{p^k}$ or $a \equiv 1 \pmod{p^k}$. Applying this to $p = 2, 5$ we get the following possibilities

- (a) $a \equiv 0 \pmod{2^k}, a \equiv 0 \pmod{5^k}$. But this implies that a is divisible by 10^k . This gives trivial solutions which are ruled out by the constraint $1 < a < 10^k$.
- (b) $a \equiv 1 \pmod{2^k}, a \equiv 1 \pmod{5^k}$. In this case $a - 1$ is divisible by 10^k , which is another trivial solution ruled out by the extra requirement $1 < a < 10^k$.
- (c) $a \equiv 0 \pmod{2^k}, a \equiv 1 \pmod{5^k}$. According to the chinese remainder theorem this has a unique residue class modulo 10^k as solution. It is not 0 or 1 modulo 10^k , hence there exists a unique solution a with $1 < a < 10^k$.
- (d) $a \equiv 1 \pmod{2^k}, a \equiv 0 \pmod{5^k}$. Again this gives a unique solution.

In all we find two solutions to our general problem.

Now let $k = 12$ according to the above we must first solve $a \equiv 0 \pmod{2^{12}}, a \equiv 1 \pmod{5^{12}}$, which gives us $a \equiv 81787109376 \pmod{10^{12}}$ and hence $a = 81787109376$. Secondly we must solve $a \equiv 1 \pmod{2^{12}}, a \equiv 0 \pmod{5^{12}}$, which gives us $a = 918212890625$. These are the two solutions.

Notice that the sum of the non-trivial solutions found above, add up to 1000000000001. Can you explain that?

- (35) Use the map $a \pmod{10} \mapsto (a \pmod{2}, a \pmod{5})$ to find

$$0 \pmod{10} \mapsto (0 \pmod{2}, 0 \pmod{5})$$

$$1 \pmod{10} \mapsto (1 \pmod{2}, 1 \pmod{5})$$

$$2 \pmod{10} \mapsto (0 \pmod{2}, 2 \pmod{5})$$

$$3 \pmod{10} \mapsto (1 \pmod{2}, 3 \pmod{5})$$

$$\begin{aligned}
4 \pmod{10} &\mapsto (0 \pmod{2}, 4 \pmod{5}) \\
5 \pmod{10} &\mapsto (1 \pmod{2}, 0 \pmod{5}) \\
6 \pmod{10} &\mapsto (0 \pmod{2}, 1 \pmod{5}) \\
7 \pmod{10} &\mapsto (1 \pmod{2}, 2 \pmod{5}) \\
8 \pmod{10} &\mapsto (0 \pmod{2}, 3 \pmod{5}) \\
9 \pmod{10} &\mapsto (1 \pmod{2}, 4 \pmod{5})
\end{aligned}$$

- (36) Case a) We must show that $4^{2^{2n+1}} \equiv 3 \pmod{13}$. Notice that the order of 4 (mod 13) equals 6. This means that in the determination of $4^k \pmod{13}$ for any k , only the value of $k \pmod{6}$ matters. So we must determine $2^{2n+1} \pmod{6}$ for all n . Note that $2^{2n+1} \equiv 0 \pmod{2}$ and $2^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{3}$ for all n . Hence $2^{2n+1} \equiv 2 \pmod{6}$. We conclude that $4^{2^{2n+1}} \equiv 4^2 \equiv 3 \pmod{13}$.

Case b) When 37 divides x , the statement is certainly true. Suppose now that 37 does not divide x . In that case, $x^{36} \equiv 1 \pmod{37}$. So we must determine $9^9 \pmod{36}$. Notice that $9^9 \equiv 0 \pmod{9}$ and $9^9 \equiv 1^9 \equiv 1 \pmod{4}$. Hence $9^9 \equiv 9 \pmod{36}$. A quick calculation shows that $x^9 \pmod{37}$ has in total 4 different values, 1, -1, 6, -6. After adding 4 to these numbers we get 5, 3, 10, -2 (mod 37). None of these numbers is 0 (mod 37).

- (37) By Euler's theorem we have

$$a^{\phi(p_i^{k_i})} \equiv a^{p_i^{k_i-1}(p_i-1)} \equiv 1 \pmod{p_i^{k_i}} \quad \text{for } i = 1, 2, \dots, r$$

Hence

$$a^{\lambda(n)} \equiv 1 \pmod{p_i^{k_i}} \quad \text{for } i = 1, 2, \dots, r$$

By the Chinese remainder theorem this implies $a^{\lambda(n)} \equiv 1 \pmod{n}$.

- (38) Notice that $2730 = 2 \times 3 \times 5 \times 7 \times 13$. By the Chinese remainder theorem it suffices to show that $n^{13} \equiv n \pmod{p}$ for all n and $p = 2, 3, 5, 7, 13$. We repeatedly use Fermat's little theorem.

$$\begin{aligned}
n^{13} &\equiv n \pmod{13} \text{ for all } n \text{ (Fermat's little theorem).} \\
n^{13} &\equiv n^7 \cdot n^6 \equiv n \cdot n^6 \equiv n^7 \equiv n \pmod{7}. \\
n^{13} &\equiv (n^5)^2 \cdot n^3 \equiv n^2 \cdot n^3 \equiv n^5 \equiv n \pmod{5}. \\
n^{13} &\equiv (n^3)^4 \cdot n \equiv n^4 \cdot n \equiv n^3 \cdot n \cdot n \equiv n^3 \equiv n \pmod{3}. \\
n^{13} &\equiv n \pmod{2} \text{ because } n \text{ is even } \iff n^{13} \text{ is even.}
\end{aligned}$$

- (43) Notice that $a^n \equiv 1 \pmod{a^n - 1}$. Furthermore, $a^k \not\equiv 1 \pmod{a^n - 1}$ for all $0 < k < n$ because $1 < a^k - 1 < a^n - 1$ for all such k . Hence the order of $a \pmod{a^n - 1}$ is precisely n . The order of an element divides the order of the group, hence $n \div \phi(a^n - 1)$.

- (44) This is slightly tedious. Write $\phi(n) = n \prod_{p|n} (1 - 1/p)$. We give a lower bound for $\prod_{p|n} (1 - 1/p)$. Notice that

$$\prod_{p|n} (1 - 1/p) \geq \frac{1}{2} \prod_{p|n, p \text{ odd}} (1 - 1/p)$$

The number of distinct primes dividing n can be at most $\log_2(n)$ (the logarithm of n in base 2). Note that for each odd prime p we have $1 - 1/p \geq 2/3$. Hence

$$\begin{aligned} \prod_{p|n} (1 - 1/p) &\geq \frac{1}{2} \left(\frac{2}{3}\right)^{\log_2(n)} \\ &= \frac{1}{2} n^{-\log(2/3)/\log(2)} \\ &\geq \frac{1}{2} n^{-0.5} \end{aligned}$$

We conclude that $\phi(n) \geq \frac{1}{2} \cdot n^{1-0.5} = \frac{1}{2} \cdot n^{0.5}$. The latter goes to ∞ as $n \rightarrow \infty$.

- (52) The orders are 6, 11, 8 respectively. To shortcut the computation, notice for example that $\phi(46) = 22$. So the order of 3 (mod 46) divides 22. Thus we need only check whether, $3^1, 3^2, 3^{11}$ are 1 (mod 46). If not, then 22 is the order of 3 (mod 46). It turns out that $3^{11} \equiv 1 \pmod{46}$.

- (53) Note that $2^p \equiv 1 \pmod{q}$. The order of 2 (mod q) thus divides p . Since p is a prime and $2^1 \not\equiv 1 \pmod{q}$ the order is precisely p . Hence p divides $\phi(q) = q - 1$. So $q \equiv 1 \pmod{p}$. Furthermore, since q is odd, $q \equiv 1 \pmod{2}$. Hence, because p is odd, we conclude that $q \equiv 1 \pmod{2p}$. So q is of the form $q = 2mp + 1$.

- (56) Trial and error shows that 2 is a primitive root modulo 11. All other primitive roots modulo 11 can then be obtained by computation of $2^k \pmod{11}$ for $1 \leq k < 10$ and $\gcd(k, 10) = 1$. So, $2^1 \equiv 2 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$, $2^9 \equiv 6 \pmod{11}$ are the primitive roots modulo 11.

From the theory it follows that 2 (mod 11^2) has order 10 or 110. Checking that $2^{10} \equiv 56 \pmod{121}$ we conclude that 2 (mod 121) has order 110 and hence is a primitive root. All other primitive roots modulo 121 can be computed by computing $2^k \pmod{121}$ with $1 \leq k < 110$ and $\gcd(k, 110) = 1$.

- (57) (a) By testing $2^d \pmod{13}$ for all divisors d of 12 we quickly see that 2 is a primitive root modulo 13. The other primitive roots are given by $2^k \pmod{13}$, where $\gcd(k, 12) = 1$. So, 2, 6, 7, 11 (mod 13).

Notice $(\mathbb{Z}/14\mathbb{Z})^* \simeq (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/2\mathbb{Z})^* \simeq (\mathbb{Z}/7\mathbb{Z})^*$. The latter group is cyclic, so there is a primitive root modulo 14. Note $\phi(14) = 6$. A quick check shows that 3 is a primitive root modulo 14. The other primitive roots are given by $3^k \pmod{14}$, where $\gcd(k, 6) = 1$. So, 3, 5 (mod 14).

Since $x^4 \equiv 1 \pmod{5}$ and $x^2 \equiv 1 \pmod{3}$ for all x with $\gcd(x, 15) = 1$, we see that $x^4 \equiv 1 \pmod{15}$ for all such x . But $\phi(15) = 8$, so there cannot be primitive roots modulo 15.

(b) Note that 5 is relatively prime with 12, the order of $(\mathbb{Z}/13\mathbb{Z})^*$. Notice that $5 \cdot 5 \equiv 1 \pmod{12}$. To solve $x^5 \equiv 7 \pmod{13}$ raise both sides to the power 5. We find, $(x^5)^5 \equiv x^{25} \equiv x \equiv 7^5 \equiv 11 \pmod{13}$. The solution is $x \equiv 11 \pmod{13}$.

In a similat way we get $x^5 \equiv 11 \pmod{14} \Rightarrow x \equiv 9 \pmod{14}$ and $x^5 \equiv 2 \pmod{15} \Rightarrow x \equiv 2 \pmod{15}$.

(58) We use the function $\lambda(n)$ from exercise 37. If we have a primitive root modulo m then we should have $\lambda(m) = \phi(m)$. In other words

$$\text{lcm}(p_1^{k_1}(p_1 - 1), \dots, p_r^{k_r}(p_r - 1)) = (p_1^{k_1}(p_1 - 1), \dots, p_r^{k_r}(p_r - 1)).$$

This means that the numbers $p_i^{k_i}(p_i - 1)$ are all relatively prime. In particular, there can be at most one odd prime factor p_i . So m is of the form $m = 2^l p^k$. When $k = 0$ we have $m = 2^l$ and we know that $l = 1, 2$. When $l = 0$ we have $m = p^k$. Suppose that $k, l > 0$ Then 2^{l-1} and $p^{k-1}(p - 1)$ are relative prime. But this is impossible if $l > 1$. Hence $l = 1$ and $m = 2p^l$.

(60) Case a) We must determine all p such that 10 has order 1,2,3,4,5 or 6 modulo 10. Hence we must determine all p that divide at least one of $10 - 1, 10^2 - 1, 10^3 - 1, 10^4 - 1, 10^5 - 1, 10^6 - 1$. This gives us $p = 3, 7, 11, 13, 37, 41, 101, 271$.

Case b) Using the idea from case a) we get $p = 239, 4649$.

Case c) $p = 73, 137$

(64) The proof is given in Theorem 5.1.7.

(65) Let $N = 3 \cdot 2^8 + 1$. The prime divisors of $N - 1$ are 2, 3. Notice that $11^{(N-1)/2} \equiv -1 \pmod{N}$ and $11^{(N-1)/2} \equiv 360 \pmod{N}$. Hence, by Lehmer's test, N is prime.

(66) Simply write down all squares $1^2, 2^2, \dots, 8^2$ modulo 17. We get 1, 4, 9, 16, 8, 2, 15, 13 (mod 17) as quadratic residues modulo 17. Similarly we get 1, 4, 9, 16, 6, 17, 11, 7, 5 (mod 19) as quadratic residues modulo 19.

(67) We first show that p does not divide b . If it did, then $p|a^2 + b^2$ and $p|b$ would imply $p|a$, which contradicts $\gcd(a, b) = 1$. Hence p does not divide b .

Now it follows from $p|a^2 + b^2$ that $a^2 \equiv -b^2 \pmod{p}$. Multiply on both sides by $b^{-2} \pmod{p}$. We get $(ab^{-1})^2 \equiv -1 \pmod{p}$. Hence -1 is a quadratic residue modulo p which implies that $p \equiv -1 \pmod{4}$.

(72) We treat two examples. First $x^2 \equiv 114 \pmod{127}$. Note that 127 is prime, so it suffices to determine $\left(\frac{114}{127}\right)$. Notice,

$$\left(\frac{114}{127}\right) = \left(\frac{2}{127}\right) \left(\frac{3}{127}\right) \left(\frac{19}{127}\right)$$

The first factor is 1 because $127 \equiv -1 \pmod{8}$. The second factor, by reciprocity equals $-\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1$. The third factor, again by reciprocity,

equals $-\left(\frac{127}{19}\right) = -\left(\frac{13}{19}\right) = -\left(\frac{19}{13}\right) = -\left(\frac{6}{13}\right)$. The latter equals $-\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -(-1)\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$. So we conclude $\left(\frac{114}{27}\right) = -1$, our equation is not solvable.

We now study the solvability of $9x^2 + 12x + 15 \equiv 0 \pmod{58}$. Splitting off squares gives $(3x + 2)^2 + 11 \equiv 0 \pmod{58}$. So it suffices to study solvability of $y^2 \equiv -11 \pmod{58}$. By the Chinese remainder theorem this is equivalent to the system $y^2 \equiv 1 \pmod{2}$, $y^2 \equiv -11 \pmod{29}$. The first equation is solvable, it remains to determine $\left(\frac{-11}{29}\right)$. Note that is equals

$$\left(\frac{-1}{29}\right)\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1.$$

Hence there are no solutions.

(73) Let p be an odd prime $\neq 5$. Note that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

The latter is 1 if $p \equiv \pm 1 \pmod{5}$ and -1 if $p \equiv \pm 2 \pmod{5}$.

Now let p be an odd prime $\neq 3$. Then

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

The latter is 1 if $p \equiv 1 \pmod{3}$ and -1 if $p \equiv -1 \pmod{3}$.

Finally,

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

we can now read off that the Legendre symbol is 1 if $p \equiv \pm 1 \pmod{12}$ and -1 if $p \equiv \pm 5 \pmod{12}$.

(69) Part a) Let a be a quadratic nonresidue modulo p and let $x = a^{(p-1)/8}$. Then, $x^4 \equiv a^{(p-1)/2} \equiv -1 \pmod{p}$.

Part b) Notice that $x^4 \equiv -1 \pmod{p}$ implies that $x^2 \equiv -x^{-2} \pmod{p}$ and hence $x^2 + x^{-2} \equiv 0 \pmod{p}$. So we find that $(x + 1/x)^2 \equiv x^2 + 2 + x^{-2} \equiv 0 \pmod{p}$. In other words, $(x + 1/x)^2 \equiv 2 \pmod{p}$ and 2 is a quadratic residue modulo p .

(74) Let $a = (-1)^{k_0} p_1 \cdots p_r$ be the prime factorisation of a where $k_0 \equiv 0$ or 1 and the primes p_i are not necessarily distinct. Note that the primes p_i are odd because $a \equiv \pm 1 \pmod{4}$. We now compute the Legendre symbol $\left(\frac{a}{p}\right)$ using quadratic reciprocity.

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{-1}{p}\right)^{k_0} \prod_{i=1}^r \left(\frac{p_i}{p}\right) \\ &= (-1)^{k_0(p-1)/2} \prod_{i=1}^r (-1)^{(p_i-1)(p-1)/4} \prod_{i=1}^r \left(\frac{p}{p_i}\right) \end{aligned}$$

Now notice the identity

$$k_0 + \sum_{i=1}^r (p_i - 1)/2 \equiv (a - 1)/2 \pmod{2}$$

On the left we simply have modulo 2 the number of primes p_i which are $\equiv -1 \pmod{4}$ and the sign of a . When this total is odd we have $a \equiv -1 \pmod{4}$, when it is even we have $a \equiv 1 \pmod{4}$. So we get

$$\left(\frac{a}{p}\right) = (-1)^{(a-1)(p-1)/2} \prod_{i=1}^r \left(\frac{p}{p_i}\right).$$

The value of the product $\prod \left(\frac{p}{p_i}\right)$ only depends on the residue class $p \pmod{|a|}$, the value of the sign depends on the parity of $(p-1)/2$. Hence $\left(\frac{a}{p}\right)$ depends only on the residue class $p \pmod{4|a|}$. Moreover, if $a \equiv 1 \pmod{4}$ the sign in front of the product is always +, so now $\left(\frac{a}{p}\right)$ depends only on the class $p \pmod{|a|}$.

(75) Note that $x^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv \left(\frac{a}{p}\right)a \equiv a \pmod{p}$.

(78) Let a be the smallest quadratic nonresidue and let b the smallest positive number such that $ab > p$. Then, $0 < ab - p < a$. Hence, by minimality of a , the residue class $ab \pmod{p}$ must be quadratic residue class. Hence b is a quadratic nonresidue. We also have $ab < p + a$, hence $b < p/a + 1$. Since also $a + 1 \leq b$ it follows that $a < p/a$ and so, $a < \sqrt{p}$.

(39) We must solve: $2^{p-1} - 1 = pu^2$ in an odd prime p and an integer u . Note that u must be odd. factorisation of the left hand side yields $(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1) = pu^2$. The factors on the left are relatively prime (check!). This implies that there exist positive integers r, s such that either

$$2^{(p-1)/2} - 1 = pr^2, \quad 2^{(p-1)/2} + 1 = s^2$$

or

$$2^{(p-1)/2} - 1 = r^2, \quad 2^{(p-1)/2} + 1 = ps^2.$$

In the first case $s^2 - 1$ is a power of 2. So $s - 1 = 2^k$ and $s + 1 = 2^l$ for certain integers k, l met $l > k > 0$. taking the difference, $2^l - 2^k = 2$. From this follows that $2^k | 2$ and hence $k = 1$. Consequently, $s = 3$ and $2^{(p-1)/2} + 1 = 8$. This gives us $p = 7$. A small check, $(2^6 - 1)/7 = 9$, a square.

In the second case we see that $r^2 + 1$ is a power of 2. Since r is odd, we have $r^2 \equiv 1 \pmod{4}$ and hence $r^2 + 1 \equiv 2 \pmod{4}$. In other words, $r^2 + 1$ contains at most one factor 2. So, $r^2 + 1 = 2 \Rightarrow r = 1 \Rightarrow 2^{(p-1)/2} - 1 = 1$. We conclude that $p = 3$. A small check, $(2^2 - 1)/3 = 1$, a square.

- (40) Wilson's theorem tells us that $(p-1)! \equiv -1 \pmod{p}$. We now rewrite the product $(p-1)!$ as

$$(p-1)! = \left(\frac{p-1}{2}\right)! \times \frac{p+1}{2} \times \cdots \times (p-1).$$

The second group of factors on the right is modulo p equal to the factors $-(p-1)/2, -(p-3)/2, \dots, -2, -1$. Hence

$$(p-1)! = (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2}\right)!\right)^2.$$

If we now notice that $(-1)^{(p-1)/2} = 1$ (because $p \equiv 1 \pmod{4}$) and $(p-1)! \equiv -1 \pmod{p}$, our assertion follows.

- (79 a)) Notice that the sum $[\sqrt{p}] + \cdots + [\sqrt{kp}]$ equals the number of lattice point, with positive coordinates, below the graph of \sqrt{px} in the interval $1 \leq x \leq k$. Notice that $[\sqrt{pk}] = [\sqrt{p(p-1)/4}] = (p-1)/2$. The graph of \sqrt{px} does not contain lattice points when $1 \leq x \leq k$. To do the counting we might as well take the number of lattice points in the rectangle $1 \leq x \leq k, 1 \leq y \leq (p-1)/2$ and the subtract the number of lattice points on the right of the graph. Hence,

$$\frac{k(p-1)}{2} - \sum_{l=1}^{(p-1)/2} \left[\frac{y^2}{p}\right].$$

Note that

$$\left[\frac{y^2}{p}\right] = \frac{y^2}{p} - \left\{\frac{y^2}{p}\right\}.$$

Take the sum for $y = 1, 2, \dots, (p-1)/2$. The first part can be summed using the formula $\sum_{l=1}^n n^2 = \frac{1}{6}n(n+1)(2n+1)$. The sum of the second part is precisely equal to K/p where K is the sum of the quadratic residues modulo p . In case $p \equiv 1 \pmod{4}$ this equals half the sum of all residue classes, which is $p(p-1)/2$.

- (80) The sum $\sum_{n \leq X} r_2(n)$ equals the number of lattice points within the disc with radius \sqrt{X} . To every lattice point (a, b) we associate the elementary square $\{(a+x, b+y) | 0 \leq x, y \leq 1\}$. Let S be the union of these squares. The number $R(X)$ is precisely equal to the surface area of S . Note that S lies within the circle with radius $\sqrt{X} + \sqrt{2}$. Note also that the circle with radius $\sqrt{X} - \sqrt{2}$ is entirely contained in S . Hence

$$\pi(\sqrt{X} - \sqrt{2})^2 \leq R(X) \leq (\sqrt{X} + \sqrt{2})^2.$$

from which we can derive that $|R(X) - \pi X| \leq 2\pi\sqrt{2X} + 2\pi$.

- (100) Part a), b) are done simply by trying. Part c) can be done by trying, but also follows from the next exercise.
- (101) We write $n = 2^k[(3/2)^k] - 1$ as sum of k -th powers. Since $n < 3^k$, it can only be written as repeated sum with terms $1^k, 2^k$. The most economic way to do this

is to use as many terms 2^k as possible. The remainder can then be written as a sum of ones. Note that $\lceil n/2^k \rceil = \lceil (3/2)^k \rceil - 1$ and the remainder after division of n by 2^k is $2^k - 1$. So we require $\lceil n/2^k \rceil - 1$ terms 2^k and $2^k - 1$ terms 1^k . Hence $g(k) \geq 2^k + \lceil (3/2)^k \rceil - 2$.

- (102) From the identity it follows that a number of the form $6m^2$ can be written as a sum of 12 fourth powers. We simply write $n = a^2 + b^2 + c^2 + d^2$ (possible by Lagrange's theorem) and use the identity.

From the hint: $n = 6N + r$ and write N as sum of four squares, we deduce that $6N$ can be written as the sum of $4 \times 12 = 48$ squares. Now choose r such that $0 \leq r \leq 5$ and write r as sum of r terms 1^4 . We conclude that $g(4) \leq 48 + 5 = 53$.

To get a refinement, note that r need not be chosen between 0 and 5. We can also choose among the remainders 0, 1, 2, 3, 3, 16, 17, each which is the sum of at most two fourth powers. Hence $g(4) \leq 48 + 2 = 50$.

- (88) We can assume that a, b, c form a Pythagorean triple. Suppose, without loss of generality, that b is even. Then there exist r, s such that $a = r^2 - s^2, b = 2rs, c = r^2 + s^2$. Hence $abc = 2rs(r^4 - s^4)$. If r or s is divisible by 5 we are done. If r, s are not divisible by 5 we have $r^4 \equiv 1 \pmod{5}$ and $s^4 \equiv 1 \pmod{5}$. Hence $r^4 - s^4 \equiv 1 - 1 \equiv 0 \pmod{5}$. So $r^4 - s^4$ is divisible by 5.

- (89) Note that x, y, z^2 is a Pythagorean triple. Assume that y is even, the case x even being similar. Then there exist $r, s \in \mathbb{N}$, with $\gcd(r, s) = 1$ and distinct parity, such that $x = r^2 - s^2, y = 2rs, z^2 = r^2 + s^2$. Note that r, s, z is again a Pythagorean triple. Now suppose r is even. Then there exist integers p, q , with $\gcd(p, q) = 1$ and distinct parity, such that $r = 2pq, s = p^2 - q^2, z = p^2 + q^2$. So we conclude that

$$x = (2pq)^2 - (p^2 - q^2)^2 = -p^4 + 6p^2q^2 - q^4, \quad y = 4pq(p^4 - q^4), \quad z = p^2 + q^2.$$

Similarly, when s is even we conclude $s = 2pq, r = p^2 - q^2, z = p^2 + q^2$ and hence

$$x = (p^2 - q^2)^2 - (2pq)^2 = p^4 - 6p^2q^2 + q^4, \quad y = 4pq(p^2 - q^2), \quad z = p^2 + q^2.$$

The remaining solutions arise from the previous ones by interchanging x and y .

- (90) From the previous problem we know that there exist integers p, q such that $abc = \pm 4pq(p^2 - q^2)(p^2 + q^2)(p^4 + p^2q^2 + q^4 - 7p^2q^2)$. Modulo 7 this equals $4pq(p^2 - q^2)(p^6 - q^6)$. When 7 divides p or q we are done. When 7 does not divide pq we have $p^6 \equiv q^6 \equiv 1 \pmod{7}$. Hence $p^6 - q^6 \equiv 1 - 1 \equiv 0 \pmod{7}$, and we are done again.

- (96) Write $4y^2 = x^3 + 1$ as $4y^2 - 1 = x^3$. Factor the left hand side, $(2y - 1)(2y + 1) = x^3$. The numbers $2y - 1, 2y + 1$ are odd and have difference 2. So they are relatively prime and from $(2y + 1)(2y - 1) = x^3$ it follows that $2y + 1 = u^3$ and $2y - 1 = v^3$ are cubes. Hence $u^3 - v^3 = 2$. The difference of two cubes can only be 2 when $u = 1, v = -1$. One way to see this is to note that $(u - v)(u^2 + uv + v^2) = 2$. Hence $u^2 + uv + v^2 = \pm 1, \pm 2$. The solutions are then found by trying.

So the final solution is $y = 0, x = -1$.

- (91) Factorisation of $x^2 + y^2 = z^3$ yields $(x + iy)(x - iy) = z^3$. We should now find the greatest common divisor d of $x + iy$ and $x - iy$. Note that d divides the sum $2x$ and the difference $2iy$. Since x, y are relatively prime we conclude that d divides 2. Hence, up to units in $\mathbb{Z}[i]$, $d = 1, 1 + i, 2$. Suppose 2 divides $x + iy$. This implies that x, y are both even, which is excluded by $\gcd(x, y) = 1$. Notice that $1 + i$ divides $x + iy$ if and only if x, y have the same parity, i.e. they are both odd. But then we have $x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod{4}$. In other words, $x^2 + y^2$ contains only one factor 2, so it can never be a square.

We conclude that $x + iy$ and $x - iy$ are relatively prime and hence $x + iy$ is, up to units, a cube in $\mathbb{Z}[i]$. So there exist $a, b \in \mathbb{Z}$ such that

$$x + iy = \epsilon(a + bi)^3$$

where $\epsilon = \pm 1, \pm i$. Note that each of these units is a cube, so we can "absorb" the unit into the cube part. Hence there exist integers a, b such that $x + iy = (a + bi)^3$. After comparison of real and imaginary part we obtain

$$x = a^3 - 3ab^2, \quad y = 3a^2b - b^3.$$

- (94) We start with the equation $2^k - 3^l = 1$. Consider the equation modulo 3. We see that $2^k \equiv 1 \pmod{3}$, hence k should be even. From the equation it follows that $2^k - 1 = 3^l$, hence $(2^{k/2} - 1)(2^{k/2} + 1) = 3^l$. Hence the factors $2^{k/2} \pm 1$ are either 1 or a power of 3. Write these factors as $3^a, 3^b$ with $b < a$ and note that their difference is 2. I.e. $3^a - 3^b = 2$. In other words, $(3^{a-b} - 1) \cdot 3^b = 2$ and we conclude that $b = 0$ and $a - b = 1$. This implies that $l = a + b = 1$ and $k = 2$. So there are no solutions $k, l \geq 2$ in this case.

Now we solve $2^k - 3^l = -1$. Consider the equation modulo 4. We find that $-3^l \equiv -1 \pmod{4}$. Hence l is even and we can proceed in a similar way as above. We get $2^k = 3^l - 1 = (3^{l/2} - 1)(3^{l/2} + 1)$. The factors $3^{l/2} \pm 1$ are either 1 or a power of 2. Write the factors as $2^a, 2^b$ with $b < a$. The difference is 2, so we get $2^a - 2^b = 2$. Hence $(2^{a-b} - 1)2^b = 2$, from which we conclude that $b = 1$ and $a - b = 1$. So $k = a + b = 3$ and $l = 2$. This is the only solution.

NOTE: Catalan's conjecture has been solved in 2002 by Michailovich

- (97) We prove the first statement by induction on n . For $n = 1$ we note that 8 divides $3^2 - 1$. For larger n we remark that $3^{2^n} - 1 = (3^{2^{n-1}} - 1)(3^{2^{n-1}} + 1)$ and use the induction hypothesis 2^{n-1} divides $3^{2^{n-1}} - 1$ and the fact that the second factor is even.

There is an error in the exercise the limit should have been $\lim_{k \rightarrow \infty} c_k / N(a_k b_k c_k) = \infty$.

We take $c_k = 3^{2^k}, a = 1, b = c_k - 1$. From the above remark we know that 2^{k+2} divides b_k . Note that

$$N(a_k b_k c_k) \leq 3N(b_k) \leq \frac{3}{2^{k+1}} b_k < \frac{3}{2^{k+1}} c_k.$$

Hence $c_k/N(a_k, b_k, c_k) > 2^{k+1}/3$. The latter tends to ∞ as $k \rightarrow \infty$.

(Extra) Show, assuming the *abc*-conjecture the modified Hall conjecture which reads as follows. For every $a < 1/2$ there exists $c(a) > 0$ such that for any positive integers x, y with $x^3 \neq y^2$ we have $|x^3 - y^2| > c(a)x^a$.

To show this we assume that $x^3 > y^2$ and define $\delta = x^3 - y^2$ and We then apply the *abc*-conjecture to $a = \delta/d, b = y^2/d, c = x^3/d$ where $d = \gcd(x^3, y^2)$. For every $\epsilon > 0$ we get

$$x^3/d < c(\epsilon)\text{rad}(x^3y^2\delta/d^3)^{1+\epsilon}.$$

Notice that $\text{rad}(x^3y^2\delta/d^3) \leq xy\delta/d$. Also notice that $y < \sqrt{x^3 - \delta} < x^{3/2}$. So we get

$$x^3/d < c(\epsilon)(xy\delta/d)^{1+\epsilon} < c(\epsilon)(x^{5/2}\delta/d)^{1+\epsilon}.$$

After multiplication by $d^{1+\epsilon}$ we obtain

$$x^3 \leq x^3d^\epsilon < c(\epsilon)(x^{5/2}\delta)^{1+\epsilon}.$$

Now choose ϵ such that $-5/2 + 3/(1 + \epsilon) = a$. Then it follows that

$$x^a < c(\epsilon)^{1/(1+\epsilon)}\delta$$

from which our assertion follows.

When $y^2 > x^3$ we put $\delta = y^2 - x^3$ and find, as above, that

$$y^{2a/3} < c(a)\delta.$$

Noticing that, by assumption, $x < y^{2/3}$, and our assertion follows also in this case.

(54) To show part (a) notice that $a^{2^n} \equiv -1 \pmod{q}$. Together with its square $a^{2^{n+1}} \equiv 1 \pmod{q}$ we note that a has order 2^{n+1} in $(\mathbb{Z}/q\mathbb{Z})^*$. Hence 2^{n+1} divides $q - 1$ which solves part (a).

We now follow a variation on Euclid's proof. Suppose there are finitely many primes p with $p \equiv 1 \pmod{2^n}$. Call them p_1, p_2, \dots, p_r . Let q be a prime divisor of $N = (2p_1p_2 \cdots p_r)^{2^n} + 1$, which is necessarily odd. Then it follows from (a) that $q \equiv 1 \pmod{2^n}$. So there is an i such that $q = p_i$. Hence $N - 1$ is divisible by q . Together with $q|N$ this gives $q|1$ which is impossible. We have a contradiction. There are infinitely many primes of the form $k \cdot 2^n + 1$.

(104) To show part (a) we expand each factor in the product as a geometric series

$$\frac{1}{1 - p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

Taking the product we see that

$$\prod_{p \leq X, p \text{ prime}} \frac{1}{1 - p^{-s}}$$

equals the sum of $\frac{1}{n^s}$ over all n which consist entirely of primes $\leq X$. This is certainly larger than the sum of $\frac{1}{n^s}$ over all $n \leq X$.

We should actually have $X > 3$ in part (b). To show part (b) one uses the integral criterion

$$\sum_{n \leq X} > \int_1^{X-1} \frac{dt}{t} = \log(X-1)$$

With a bit more care we can also get the lower bound $\log(X)$:

$$\sum_{n \leq X} > 1 + \int_2^{X-1} \frac{dt}{t} = 1 - \log(2) + \log(X-1) > \log(X).$$

From (a) and (b) with $s = 1$ it follows that

$$\prod_{p \leq X, p \text{ prime}} \frac{1}{1-p^{-1}} > \log(X).$$

Take logs on both sides

$$\sum_{p \leq X, p \text{ prime}} -\log(1-p^{-1}) > \log \log(X).$$

Some calculus shows that $-\log(1-x) < x + 4x^2/5$ for all $x \in [0, 1/2]$. Hence

$$\sum_{p \leq X, p \text{ prime}} \frac{1}{p} + \frac{4}{5p^2} > \log \log(X).$$

Notice also that the sum of $1/p^2$ over all primes p can be bounded above by the sum of $1/n^2$ over all integers $n \neq 1, 4$. The latter sum equals $\pi^2/6 - 1 - 1/16 = 0.58\dots$. Times $4/5$ this yields a number $< 1/2$. So we get

$$\frac{1}{2} + \sum_{p \leq X, p \text{ prime}} \frac{1}{p} > \log \log(X)$$

as desired.

(106) Notice that

$$\begin{aligned} \prod_{p \text{ prime}} \frac{p^2+1}{p^2-1} &= \prod_{p \text{ prime}} \frac{p^2-1}{(p^2-1)^2} \\ &= \prod_{p \text{ prime}} \frac{1-p^{-4}}{(1-p^{-2})^2} \\ &= \frac{\zeta(2)^2}{\zeta(4)} = \frac{(\pi^2/6)^2}{\pi^4/90} = \frac{5}{2}. \end{aligned}$$

(107) Notice that, by definition, $n = \pi(p_n)$. Hence, by the prime number theorem,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \frac{p_n}{\log(p_n)} = 1.$$

It now remains to show that

$$\lim_{n \rightarrow \infty} \frac{\log(p_n)}{\log(n)} = 1.$$

This follows from the fact that for sufficiently large n we have

$$\frac{1}{2} \frac{p_n}{\log(p_n)} < n < 2 \frac{p_n}{\log(p_n)},$$

which implies

$$\log(p_n) - \log \log(p_n) - \log(2) < \log(n) < \log(p_n) - \log \log(p_n) + \log(2).$$

After division by $\log(n)$ and letting $n \rightarrow \infty$ we find the desired limit.

(109) From the previous exercise we know that p_n , the n -th prime is asymptotic to $n \log(n)$. In particular, for sufficiently large n , $p_n > n \log(n)/2 > \sqrt{n}$. So we get

$$\sum_{p \text{ prime}} \frac{1}{p \log(p)} < \text{finite part} + \sum_{n \text{ large}} \frac{2}{n \log(n) \cdot \log(n)/2}.$$

The latter infinite series converges by the integral criterion.

Similarly we have for sufficiently large n that $p_n < 2n \log(n) < n^2$. Hence

$$\sum_{p \text{ prime}} \frac{1 \log(p)}{p} > \text{finite part} + \sum_{n \text{ large}} \frac{2 \log(n)}{n \log(n)/2}.$$

The latter infinite series is the harmonic series which diverges.

(116) Suppose that $e + \pi$ and $e\pi$ are rational. Then the polynomial $(X - e)(X - \pi)$ has rational coefficients. Hence its zeros e, π would be quadratic numbers, contradicting the fact that e is transcendental.

(117) Suppose the series has a rational value, say p/q . Choose k and consider the difference

$$\delta = \frac{p}{q} - \sum n = 0^k \left(\frac{4}{5}\right)^n \frac{1}{3^{n^2}}.$$

This is a non-zero rational number with denominator dividing $q5^k3^{k^2}$. So we get that $\delta \geq \frac{1}{q}5^{-k}3^{-k^2}$. On the other hand we have

$$\delta = \sum_{n=k+1}^{\infty} \left(\frac{4}{5}\right)^n \frac{1}{3^{n^2}}.$$

Let us estimate the terms of this series by $(4/5)^n 3^{-(k+1)^2}$. Hence

$$\delta < \sum_{n=k+1}^{\infty} (4/5)^n 3^{-(k+1)^2} < 3^{-(k+1)^2} \sum_{n=0}^{\infty} (4/5)^n = 5 \cdot 3^{-(k+1)^2}.$$

Comparison of the bounds show that

$$\frac{1}{q} 5^{-k} 3^{-k^2} < 5 \cdot 3^{-(k+1)^2}.$$

Multiplication by 3^{k^2} gives us $\frac{1}{q} 5^{-k} < 5 \cdot 3^{-2k-1}$, hence $(9/5)^k < 5q/3$. This is impossible if we choose k big enough. Hence our number is irrational.