Computer Science Tripos Part 1A
Mathematical Tripos Part 1A (CS option)

Discrete Mathematics

Solutions to exercises

A1 - Integers

1. Induction.
2. $[n(n+1)/2]^2$.
3. $1 - 1/(n+1)!$.
4. $2^{4n+6} + 3^{2n+3} = 16.(2^{4n+2} + 3^{2n+1}) - 7.3^{2n+1}$,
   $3^{n+2} + 4^{2n+1} = 3.(3^{n+1} + 4^{2n-1}) + 13.4^{2n-1}$,
   or use modular arithmetic.
5. Induction (or solve directly as a second-order, homogeneous, linear difference equation).
6. Induction.
7. P(n) = "A $2^n \times 2^n$ chessboard with one purple square can be covered by triominoes".
8. The key to cell number n has been turned once for every factor of n, so the door will be left unlocked if n has an odd number of factors. The factors of n can be paired off unless n is a square.
9. Don't be frightened by the notation. Base case has n=0 so S=Ø. For the inductive step, let P_n be the product for $S=\{1,2,\ldots,n\}$. $P_{n+1}=(1+x_{n+1})P_n$. $1.P_n$ gives the subsets of S_{n+1} that do not contain n+1 and $x_{n+1}P_n$ gives the subsets that do.
10. By counting, the most extrovert guest shook 2n hands and the most timid shook none. The former shook hands with everyone apart from sibself and sis spouse. It follows that the maximal and minimal shakers were married to each other. Given that neither was the Master, the other could not have been the Master's wife. Uninvite them.
11. P(n) = "$n \in L$".
12. Ho, ho…

A2 – Factors

1. No, no, yes.
2. 57.17 – 44.22 = 1 and 57.44 – 44.57 = 0.
3. No.
   x = 437k – 308, y = 234 – 332k.
4. X = -31, y = 31, z = -3.
5. 25.
6. a|a and (a,b)|b so a.(a,b)|a.b and a|m. Write a = c.(a,b) and b = d.(a,b), and remember that (c,d) = 1. a|n so write n = e.a = e.c.(a,b), and write n = f.d.(a,b) similarly. Now m = a.b/(a,b) = c.d.(a,b) and n/(a,b) = e.c = f.d. c|n/(a,b) and d|n/(a,b), but (c,d) = 1 so c.d | n/(a,b) and m = c.d.(a,b) |n.
7. $4 = 2.2 = (\sqrt{5}+1)(\sqrt{5}-1)$.
8. Suppose there are only finitely many primes of the form 4k+3. Let p_n be the largest of them and calculate N as in the question. N may be composite but its prime factors are all greater than p_n and so they are all congruent to 1 modulo 4. So their product, N, is also congruent to 1 modulo 4. But it isn't.
9. Wlog, suppose (d,e)=k>1. Then k|f as well. d and e can not both be even (else f would be even giving a common factor of 2). d and e can not both be odd (else $d^2+e^2 \equiv 2 \pmod 4$ which could not be f^2). d odd and e even makes f odd, so f+d and f-d are both even. $4g^2 = e^2 = f^2-d^2 = (f+d)(f-d) = 2h.2i = 4hi$. (h,i)|(h+i)=f and (h,i)|(h-i)=d but (f,d)=1. Consider prime factorization of g^2.

10. Induction on k.
    $f_{ln} = f_n\, f_{(l-1)n+1} + f_{n-1} f_{(l-1)n}$ and use induction on l.
    $(f_n, f_{n-1}) = (f_{n-1}, f_{n-2}) = \ldots = (f_2, f_1) = (1, 1) = 1$.
    $f_m = f_n\, f_{m-n+1} + f_{n-1}\, f_{m-n}$. Consider factors and replicate derivation of Euclid's algorithm.
    $f_m \mid f_{mn}$ and $f_n \mid f_{mn}$ by above, but $(f_m, f_n) = f_{(m, n)} = f_1 = 1$, so $f_m\, f_n \mid f_{mn}$.
11. Worth thinking about efficiency: only test for odd factors (beyond 2), stop at $\sqrt{n}$, keep a list of primes and only test for divisibility by them…
12. Define a function that takes two triples (r, s, t) from the extended Euclid's algorithm and returns the next one.

A3 – Modular arithmetic

1. $10 \equiv 1 \pmod 9$ so $10^k \equiv 1 \pmod 9$ and $\Sigma d_k 10^k \equiv \Sigma d_k \pmod 9$.
2. $10 \equiv -1 \pmod{11}$ so $10^k \equiv (-1)^k \pmod{11}$ and $\Sigma d_k 10^k \equiv \Sigma(-1)^k d_k \pmod{11}$.
3. $\sum_{k=0}^{9} k = 45 \equiv 0 (\mathrm{mod}\, 9)$ but $100 \equiv 1 \pmod 9$.
4. 1 (99 = 9.11).
5. A transposition of digits k and k+1 from de to ed makes a difference of $[dk + e(k+1)] – [ek + d(k+1)] = e – d$ to the weighted sum. A change from dde to dee makes a difference of (d-e)k. A base of 10 would mask errors where d-e = 2 and k = 5.
6. Consider mod 2.
7. $x \equiv 23 \pmod{40}$.
   $y \equiv 7 \pmod 9$.
   $z \equiv 12 \pmod{17}$ so $z \equiv 97 \pmod{357}$.
8. 408.
9. $21! \equiv 1 \pmod{23}$ as in the proof of Wilson's Theorem. $21^{22} \equiv 1 \pmod{23}$ by Fermat. $21 \equiv -2 \pmod{23}$ and $2.12 = 24 \equiv 1 \pmod{23}$ so $21.11 \equiv (-2).(-12) \equiv 1 \pmod{23}$. $20!\ 21^{20} \equiv 11^3 \equiv 20 \pmod{23}$.
10. $a^{256} \equiv 1 \pmod{257}$ by Fermat and $256 = 2^8 \mid 10^9$ so $a^{1000000000} \equiv 1 \pmod{257}$.
11. Observe 42 = 2.3.7 and observe $n^7 \equiv n \pmod p$ for p = 2, 3 and 7.
12. 3901 = 47.83. $1997.17 \equiv 1 \pmod{46.82}$. only_eight_more_terms!
13. If $a = kp^i$ then $a \equiv 0 \pmod p$ so $a^{de} \equiv 0 \pmod p$. However $a^{de} = a.a^{-\varphi(p)\varphi(q)c} \equiv a.1^{-\varphi(p)c} \pmod q = a$. Use the Chinese Remainder Theorem.
14. Not all numbers are squares modulo 11. In particular, 6 is not.

A4 – Tripos questions

CST 1998 Paper 1 Question 7 (Note that there was a misprint in the published version of this question.)

CRT – bookwork.

Decoding – $ap \equiv 1 \pmod{q-1}$ so $ap = k(q-1) + 1$. Now $s^a = m^{pqa} \equiv (m(^{q-1)k}\ m)^q \equiv m^q \equiv m \pmod q$. $s^b \equiv m \pmod p$ similarly. Now use CRT to recover m (mod pq=n).

CST 1999 Paper 1 Question 2

If n = a.b with a, b > 1, then $2^n – 1 = (2^b - 1)(2^{n-b} + 2^{n-2b} + 2^{n-3b} + \ldots 2^{n-ab})$.

$\Delta_p = p.2^{n-1}$ and so has proper factors $1, 2, 2^2, 2^3, \ldots, 2^{n-1}, p, 2p, 2^2p, 2^3p, \ldots, 2^{n-2}p$ whose sum is $2^n-1 + (2^{n-1}-1)p = 2^{n-1}p = \Delta_p$.

CST 1999 Paper 1 Question 7

$\varphi(n) = |\{ x \in \mathbb{N} \mid 1 \le x < n \text{ and } (x, n) = 1 \}|$ where (x, n) denotes the highest common factor of x and n.

Suppose n > 1 and (n, a) = 1. Let U_n = { x∈ ℕ | 1 ≤ x < n and (x, n) = 1 } be the set of units modulo n. Say $U_n = \{u_1, u_2, \ldots, u_f\}$ where f = φ(n). Observe a ∈ U_n so $a.u_1, a.u_2, \ldots, a.u_f$ are all in U_n. Moreover, they are distinct because $a.u_i = a.u_j \Rightarrow n \mid a.(u_i - u_j)$, so $u_i = u_j$. Hence $\{a.u_1, a.u_2, \ldots, a.u_f\} = U_n = \{u_1, u_2, \ldots, u_f\}$. Consider the products of the elements in the two sets: $a^f u_1u_2 \ldots u_f = u_1u_2 \ldots u_f$. Units have multiplicative inverses modulo n and so can be divided away leaving $a^f \equiv 1$ (mod n)

Given a prime p, φ(p) = p-1, and a < p means that (p, a) = 1. Hence p divides a^{p-1}-1.

Let a = 10 so (p, a) = 1 and p | 10^{p-1}-1. Consider $10^{k(p-1)}$-1 for k = 1, 2, …. Each has 9s as all its digits and is divisible by 10^{p-1}-1, and so is divisible by p.

CST 2000 Paper 1 Question 8

(2u,2v) = 2.(u,v), (2u,2v+1) = (u, 2v+1), (2u+1,2v) = (2u+1,v), (u,v) = (u-v,u) = (u-v,v).

Invariant starts as (a,b).1 and ends as (a,a).c = a.c which is the final value returned.

u.v ≤ 2u.2v/2, u.(2v+1) ≤ 2u.(2v+1)/2, (2u+1).v ≤ (2u+1).2v/2, (u-v)(2v+1) = (2u-2v)(2v+1)/2 ≤ (2u+1)(2v+1)/2.

If a < 2^n and b < 2^n then a.b < 2^{2n} and the algorithm concludes in at most 4n steps. Hence O(log a).

CST 2001 Paper 1 Question 2

Existence: Use contradiction. Pick a minimal counter-example. Either it is prime and we are done or it can be factored into two smaller numbers which consequently have expressions.

Uniqueness. Use contradiction. Pick a minimal counter-example and express it as two different products of powers of primes. Pick a prime in the first expression. It must appear in the second so divide by it to give two expressions for a smaller number, which must be the same.

Any factor of *n* must consist of a product of lower powers of the same primes.

36 = $2^2 3^2$, so α_1=1, α_2=1, α_3=2 and α_4=2, and the smallest number will be $2^2 3^2 5^1 7^1$ = 1260.

CST 2001 Paper 1 Question 7

Given $m \geq 2$ and a with $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod m$ where $\varphi(m)$ is Euler's totient function.

If there is a value $a \leq p$ for which $a^{p-1} \neq 1 \pmod p$, then p is <u>not</u> prime.
(3-1)|(561-1), (11-1)|(561-1) and (17-1)|(561-1) so $a^{(561-1)} \equiv 1$ (mod 561) for all a by the CRT. Consider $a^{(p-1)/2} \neq \pm 1 \pmod p$ instead.

Pick primes p and q with product m so $\varphi(m) = (p-1)(q-1)$. Pick e and d with $ed \equiv 1 \pmod{\varphi(m)}$. Then $(a^e)^d \equiv a \pmod m$. Publish m and e while keeping d secret.

Suppose $de - 1 = n\ \varphi(m)$. n can be found by rounding up $(de - 1)/m$. Hence calculate $\varphi(m)$. p and q are the roots of $x^2 - (m + 1 - \varphi(m))x + m = 0$.

CST 2002 Paper 1 Question 7

Fermat & Diffie-Hellman: bookwork.

Montgommery: B is a power of 2 and p is odd, so they are co-prime and B has a reciprocal (mod p).
Therefore m has inverse $m^{-1}(u) \equiv uB^{-1} \pmod p$.
$m(x \times y) \equiv xyB \pmod p = xB\ yB\ B^{-1} \pmod p \equiv m^{-1}(m(x) \times m(y))$.
$u + vp \equiv u - up^{-1}p \pmod B$ $vp \equiv u - u = 0$, so $u + vp$ is a multiple of B.
$x = (u + vp)\ B^{-1} \equiv uB^{-1} \pmod p$.
$u < pB$ and $v < B$ so $u + vp < 2pB$ and $x < 2p$. But we then subtract p from x if $x \geq p$, leaving $x < p$.
$x \equiv uB^{-1} \pmod p$ and $x < p$ so $x = m^{-1}(u)$.

B1 – Sets

1. {1, 2, 3, 5} and {3}.
   1, 5} and {2}.
   {1, 5} and {1, 2, 3, 5}.
   {1, 2, 5}.
   {(1,2), (1,3), (3,2), (3,3), (5,2), (5,3)}, vice versa and $\varnothing$.
   {(0,1), (0,3), (0,5), (1,2), (1,3)}, vice versa and {(0,1), (0,3), (0,5)} $\approx$ A.
2. Yes, no, no, yes, no, no, yes.
3. Everybody loves somebody but there is not necessarily a single person who is loved by everyone else (or that person wouldn't be single, presumably…).
4. m.n, m + n, 2^m.
5. 32.
6. Let A_k be the number of permutations (deliveries of n letters) that result in letter k being correctly delivered.
   We are interested in deliveries in the complement of the union of the A_k.
   Let p_k be the number of permutations of n letters that result in at least k of them being correctly delivered.
   To calculate p_k, consider the number of ways of permuting the remaining (n-k) letters and the number of ways of choosing the k fixed letters from n.
   Observe that the answer tends to e^{-1} as n becomes large.
7. a $\oplus$ b.
8. Just do it.
9. $\{[(a \vee \sim k) \Rightarrow g] \wedge [g \Rightarrow w] \wedge \sim w\} \Rightarrow k$ which simplifies to true.

B2 – Relations

1. {(2,z), (3,x), (3,z)}.
2. R $\cup$ {(3,3)}.
   R $\cup$ {(2,4)}.
   2R3 & 3R2 but $2 \neq 3$.
   R $\cup$ {(3,3), (4,3)}.
3. 2^{km} and 2^{kmn}.
4. {{1}, {2}, {3}}, {{1,2}, {3}}, {{1,3}, {2}}, {{1}, {2,3}}, {{1,2,3}}. 5. $2^{3.3} = 512$.
5. $(y,x) \in (R\cap S)^{-1} \Leftrightarrow (x,y) \in R\cap S \Leftrightarrow (x,y) \in R \wedge (x,y) \in S \Leftrightarrow (y,x) \in R^{-1} \wedge (y,x) \in S^{-1} \Leftrightarrow (y,x) \in R^{-1}\cap S^{-1}$.
   Similarly.
6. A = {1, 2} and R = {(1,2), (2,1)}.
7. R is reflexive and $R \subseteq R \cup S \subseteq t(R\cup S)$ so that is reflexive too.
   $(x,y) \in t(R\cup S) \Rightarrow \exists\, x_0 = x, x_1, x_2, \ldots x_n = y$ with $(x_i,x_{i+1}) \in R\cup S$ for $0 \le I < n$. If $(x_i,x_{i+1}) \in R$ then $(x_{i+1},x_i) \in R$ and if $(x_i,x_{i+1}) \in S$ then $(x_{i+1},x_i) \in S$, so $(x_{i+1},x_i) \in R\cup S$. Hence $(y,x) \in t(R\cup S)$.
   Clearly t(R∪S). is transitive, so it is an equivalence relation.
   Moreover, any equivalence relation containing R∪S must contain t(R∪S) so that is the smallest such.
8. r(R) – treat 1 as a prime. s(R) – x is a multiple or divisor of y by a prime amount. t(R) – x is a strict factor of y.
   Yes, yes, no (t(s(R)) is reflexive but s(t(R)) need not be).
   Yes, yes, no.
   t(s(r(R))).
   Divisibility order. No – symmetry precludes anti-symmetry in general.
9. Diagonal order and lexicographic order.

B3 – Functions

1. $2^2 = 4$, $2^3 = 8$, $3^2 = 9$ and $3^3 = 27$.
2. $[X] \leftrightarrow X \cap B$. $[X] = [Y] \Leftrightarrow X \cap B = Y \cap B$.
3. Bijective.
4. $(a, (b,c)) \leftrightarrow ((a,b), c)$.
   Requires $|A| = 0$, 1 or ∞.
   Requires $|A| = 0$, 2 or ∞.
   Currying.
   $|C| = 1$ or $|B|^{|A|} = |B|.|A|$.
   $(f\colon A+B \to C) \leftrightarrow (\lambda a.f(0,a), \lambda b.f(1,b))$.
5. Suppose $\exists$ g with p o g = f o q. $a_1 R a_2 \Rightarrow [a_1]=[a_2] \Rightarrow p(a_1)=p(a_2) \Rightarrow g(p(a_1))=g(p(a_2)) \Rightarrow q(f(a_1))=q(f(a_2)) \Rightarrow [f(a_1)]=[f(a_2)] \Rightarrow f(a_1) \mathrel{S} f(a_2)$.
   Define $g([a]) = q(f(a))$ which is well defined everywhere and satisfies. P o g = f o q.
6. Consider Hasse diagrams.
7. $(|B|+1)^{|A|}$.
8. Countable union of finite sets.
9. $f \leftrightarrow \{n \mid f(n) = 1\}$.
10. Countably infinite, uncountable, finite (=2), uncountable, countable.
11. Each disc contains a point with rational coordinates.
    Circles can be nested arbitrarily.

B4 – Tripos questions

CST 1998 Paper 1 Question 2

$R \subseteq A \times A$.
Refelxive, symmetric, transitive.
$\cup [a] = A$, $[a] \cap [b] \neq \varnothing \Rightarrow [a] = [b]$.
n = 0, natural numbers.

CST 1998 Paper 1 Question 8

$R \subseteq A \times A$; reflexive, anti-symmetric, transitive; $\forall a,b \in A . aRb \vee bRa$; bookwork…
Effectively product order; consider decimal expansions.

CST 1999 Paper 1 Question 8

Reflexive by considering identity function. Symmetric since inverse of bijection is a bijection. Transistive because composition of bijections is a bijection.

A is countable if $A \cong N$, the natural numbers, (or if A is finite).

Given injections $A \to B$ and $B \to A$, $\exists$ a bijection $A \to B$.

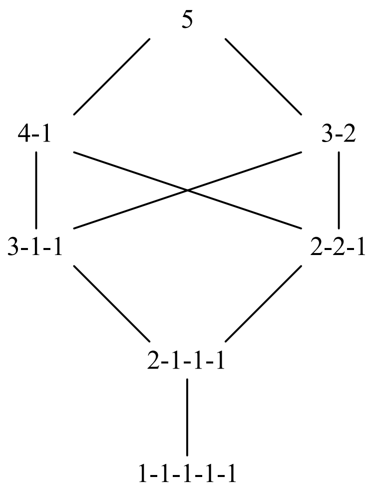
$z \to 2z + 1$ if $z > 0$, $-2z$ otherwise. $a/b \to 2^a 5^b$ if $a > 0$, $3^{-a}5^b$ otherwise and use S-B. Show P(N) uncountable by contradiction, construct injection $P(N) \to R$ by $\{a_i\} \to \Sigma\, 10^{-ai}$ and use S-B for contradiction.

Let A_n be the programs of length n and so finite. Countable union of finite sets is countable.

CST 2000 Paper 1 Question 2

Reflexive, anti-symmetric and transitive.

Reflexive: $k_i = i$. Anti-symmetric: two partitions must have same number of elements so only one term in each sum. Transitive: substitute one decomposition into the other.



CST 2000 Paper 1 Question 7

Every infinite descending sequence of elements is ultimately constant.

$(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow (a_1 <_A a_2) \vee ((a_1 = a_2) \wedge (b_1 \leq_B b_2))$. Bookwork.

N×N with the lexicographic order: (1,1) is separated from (2,1) which is separated from (3,1) and so on.

Take any pair of elements x and y. Wlog $x < y$. x and y are separated, so find z_1 with $x < z_1 < y$. Now x and z_1 are separated, so find z_2 with $x < z_2 < z_1$. Hence form an infinite descending sequence.

CST 2001 Paper 1 Question 8

$(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow (a_1 \leq_A a_2) \wedge (b_1 \leq_A b_2)$. Reflexive, anti-symmetric and transitive.

Lowest common multiple and greatest common divisor.

Union and intersection.

$\mathbb{N}$ itself has no least upper bound. Otherwise yes. 0 is LUB for $\mathbb{N}_0$.

LUB of pair is pair of LUBs and so on.

CST 2002 Paper 1 Question 2

No infinite descending sequences of elements.

Use contradiction. Construct an infinite descending sequence of elements.

Choose shortest u with au = ub, and write u = av. Then aav = avb so av = vb with |v| < |u|.

CST 2002 Paper 1 Question 8

Suppose $x \in (\cap_{B\in\mathbf{B}}B)\cup(\cap_{c\in\mathbf{C}}C)$. Then either $\forall B\in\mathbf{B}.x\in B$ or $\forall C\in\mathbf{C}.x\in C$. In both cases $\forall B\in\mathbf{B}.\forall C\in\mathbf{C}.x\in B\cup C$ so $x\in\cap_{(B,C)\in\mathbf{B}\times\mathbf{C}}(B\cup C)$.

Suppose $x\in\cap_{(B,C)\in\mathbf{B}\times\mathbf{C}}(B\cup C)$. Then $\forall B\in\mathbf{B}.\forall C\in\mathbf{C}.x\in B\cup C$ so $\forall B\in\mathbf{B}.x\in B\cup)\cup(\cap_{c\in\mathbf{C}}C)$. Hence $x\in(\cap_{B\in\mathbf{B}}B)\cup(\cap_{c\in\mathbf{C}}C)$.

Suppose $C\in\mathbf{A}$ and $(X,y)\in\mathbf{R}$ with $X\subseteq C$. Then $y\in C$ by the definition of $\mathbf{R}$, and so C is $\mathbf{R}$-closed.

Suppose C is $\mathbf{R}$-closed. Let $\mathbf{B}=\{A\in\mathbf{A}|C\subseteq A\}$ so $\mathbf{B}\subseteq\mathbf{A}$. Then $\forall B\in\mathbf{B}.C\subseteq B$ so $C\subseteq\cap_{B\in\mathbf{B}}B$. On the other hand, if $x\in\cap_{B\in\mathbf{B}}B$, then $\forall A\in\mathbf{A}$ with $C\subseteq A$ we have $x\in A$, so $(C,x)\in\mathbf{R}$. But C is $\mathbf{R}$-closed, so $x\in C$. Therefore $C = \cap_{B\in\mathbf{B}}B \in \mathbf{A}$ since $\mathbf{A}$ is intersection-closed.