8036 Semester 2 2011

The University of Sydney

FACULTY OF SCIENCE

MATH2068 and MATH2988

Number Theory and Cryptography

November, 2011

Lecturer: R. B. Howlett

Time allowed: two hours

The question paper must not be removed from the examination room

No notes or books are to be taken into the examination room.
Only approved non-programmable calculators are allowed.

The MATH2068 paper has five questions.
The MATH2988 paper has one extra question (on the back page).
The questions are of equal value.

Question 6 is for MATH2988 only.

. . . /2

1. (*i*) Use a Vigenère cipher with keyword CAT to encrypt the plaintext message OCELOT.

(*ii*) Let $M = c_1c_2c_3\ldots c_\ell$ be a message which is a sequence of letters from the alphabet $\{\mathrm{A},\mathrm{B},\ldots,\mathrm{Z}\}$.

(a) What is a *digraph*, and what is the definition of the *digraph coincidence index of* M?

(b) If the sequence M were generated by choosing successive letters independently with all letters having equal probability of being chosen each time, what would be the expected value of the digraph coincidence index?

(c) If M is ordinary English text, written in upper case letters and stripped of spacing and punctuation, would you expect the digraph coincidence index to be greater than, less than, or the same as the answer to Part (*ii*) (b)? (Give a brief reason.)

(*iii*) A long intercepted message M is reliably known to have been encrypted with a block transposition cipher. If the $(2,7)$-decimation of M with period 9 has coincidence index 0.0047 and the $(3,5)$-decimation of M of period 8 has coincidence index 0.0072, what conclusions should you draw?

Solution: (*i*)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

plaintext:	14	2	4	11	14	19
key:	2	0	19	2	0	19
ciphertext:	16	2	23	13	14	12

Thus encryption produces QCXNOM.

(*ii*) (a) A digraph is a pair of adjacent letters. The digraph coincidence index of M is the probability that two randomly chosen digraphs of M coincide. (More exactly, for each x and each y in the alphabet $\{\mathrm{A},\mathrm{B},\ldots,\mathrm{Z}\}$ let n_{xy} be the number of occurrences of xy as a digraph of M: thus n_{xy} is the number of elements of the set $\{\, i \in \mathbb{Z} \mid 1 \le i \le \ell-1 \text{ and } (c_i, c_{i=1}) = (x,y) \,\}$. Then the digraph coincidence index of M is $\sum_{x,y}(n_{xy}/(\ell-1))^2$, where the sum is over all 26^2 possible values of (x,y).)

(b) The expected value of the probability that a randomly chosen digraphs equals a given digraph xy is $(1/26)^2$, and so the expected value of the probability that two randomly chosen digraphs both equal xy is $(1/26)^4$. The expected value of the digraph coincidence index is therefore $\sum_{x,y}(1/26)^4 = (1/26)^2$, since there are 26^2 possible values for (x,y).

(c) If M is a piece of ordinary English then the frequency distribution of the digraphs of M will be uneven, in the sense that the frequency of some digraphs will be much greater than $(1/26)^2$ and the frequency of others will be much less than $(1/26)^2$. The result is that the digraph coincidence index will be much larger than the $(1/26)^2$ of (b) above. (The minimum value of $\sum_{i=1}^{k} p_i^2$ subject to the constraint that all p_i are nonnegative and $\sum_{i=1}^{k} p_i = 1$ occurs when all p_i equal $1/k$.)

(*iii*) You should conclude that the block length for the cipher is 8 and that when the ciphertext is split into eight-letter blocks the third and fifth letters of each block were originally adjacent letters of the plaintext.

2. (*i*) An *affine cipher* is a substitution cipher defined by a rule of the form

$$i \mapsto mi + n \pmod{26},$$

for some fixed integers m, n, where the letters A to Z are identified with residues modulo 26 in the usual way (A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, etc.). The pair (m, n) is called the *key*.

(a) If the key is $(8, 16)$, encipher the message BEN.

(b) A sample of ciphertext known to have been produced by an affine cipher is found to consist of 2000 letters altogether, of which the two most common are J (271 occurrences) and N (199 occurrences). Assuming that these represent the most common letters in English, determine the key.

(*ii*) Let $n = (d_\ell d_{\ell-1} \dots d_0)_8$; that is, when the integer n is expressed in base 8 notation its digits are d_ℓ, $d_{\ell-1}$, $\dots$, d_0.

(a) Explain what this means, and illustrate your answer by finding the base 10 representation of $n = (2145)_8$.

(b) Prove that $n \equiv d_0 + d_1 + \cdots + d_\ell \pmod 7$.

Solution: (*i*) (a) Numerically BEN is (1,4,13). Now

$$\begin{aligned} 8 \times 1 + 16 &= 24 \\ 8 \times 4 + 16 &= 48 \equiv 22 \pmod{26} \\ 8 \times 13 + 16 &= 120 \equiv 16 \pmod{26} \end{aligned}$$

and converting (24,22,16) back into letters produces YWQ.

(b) Note that numerically J $\leftrightarrow$ 9 and N $\leftrightarrow$ 13. The most common letter of English is E $\leftrightarrow$ 4 and the second most common is T $\leftrightarrow$ 19. So we need to find m and n such that

$$4m + n \equiv 9 \pmod{26}, \tag{1}$$
$$19m + n \equiv 13 \pmod{26}. \tag{2}$$

Subtracting (1) from (2) gives $15m \equiv 4 \pmod{26}$, whence $15m \equiv 30 \pmod{26}$. By coprime cancellation this gives $m \equiv 2 \pmod{26}$, and substituting back into (1) gives $n \equiv 1 \pmod{26}$. So the key is $(m, n) = (2, 1)$.

(*ii*) (a) The notation means that $n = d_\ell 8^\ell + d_{\ell-1}8^{\ell-1} + \cdots + d_1 8^1 + d_0 8^0$. Thus $(2145)_8 = 2 \times 8^3 + 8^2 + 4 \times 8 + 5$, which is 1125 in base 10 notation.

(b) Since $8 \equiv 1 \pmod{7}$ and congruence respects addition and multiplication, it follows that $8^k \equiv 1^k \equiv 1 \pmod{7}$ for all nonnegative integers k, and

$$n \equiv d_\ell 1^\ell + d_{\ell-1}1^{\ell-1} + \cdots + d_1 1 + d_0 \equiv d_0 + d_1 + \cdots + d_\ell \pmod{7},$$

as required.

3. (*i*) Find the order of 4 modulo each of the primes 11 and 23, and then find the residue of 4^{1112} modulo 253. (You are given that $253 = 11 \times 23$.)

(*ii*) Prove that if n, a and b are integers such that $n|ab$ and $\gcd(n, a) = 1$ then $n|b$. You may use the fact that integers r and s exist satisfying $rn + sa = \gcd(n, a)$.

(*iii*) Show that if p is a prime number and t an integer such that $t^2 \equiv 1 \pmod{p}$, then either $t \equiv 1 \pmod{p}$ or $t \equiv -1 \pmod{p}$.

Solution: (*i*) If p is any odd prime then $4^{(p-1)/2} = 2^{p-1} \equiv 1 \pmod{p}$, by Fermat's Little Theorem, and so $\mathrm{ord}_p(4)$ must be a divisor of $(p-1)/2$. Since $\mathrm{ord}_p(4)$ can only be 1 if $p|(4-1) = 3$, it follows that $\mathrm{ord}_{11}(4) = 5$ and $\mathrm{ord}_{23}(4) = 11$.

Write N for the residue of 4^{1112} modulo 253. Since $\mathrm{ord}_{11}(4) = 5$ it follows that if n and m are arbitrary nonnegative integers then $4^n \equiv 4^m \pmod{11}$ if and only if $n \equiv m \pmod{5}$. So $N \equiv 4^{1112} \equiv 4^2 \equiv 5 \pmod{11}$, giving $N = 11k + 5$ for some integer k. Similarly $4^n \equiv 4^m \pmod{23}$ if and only if $n \equiv m \pmod{11}$, and since $1112 \equiv 1 \pmod{11}$ it follows that $N \equiv 4^{1112} \equiv 4 \pmod{23}$. Hence

$$11k + 5 \equiv 4 \pmod{23}$$

and therefore

$$11k \equiv -1 \equiv 22 \pmod{23}$$

and coprime cancellation yields $k \equiv 2 \pmod{23}$. So $k = 23h + 2$ for some integer h, and hence

$$N = 11k + 5 = 11(23h + 2) + 5 = 253h + 27.$$

Since $0 \leq N < 253$ it follows that $N = 27$.

(*ii*) Assume that n, a and b are integers such that $n|ab$ and $\gcd(n, a) = 1$. Since $\gcd(n, a) = 1$ there exist integers r and s such that $rn + sa = 1$, and multiplying through by b gives $rnb + sab = b$. Since $n|ab$ there exist an integer t such that $ab = tn$, and so it follows that

$$b = rnb + sab = rbn + stn = (rb + st)n.$$

Since r, b, s and t are all integers, so is $rb + st$. Hence $n|b$, as required.

(*iii*) Assume that p is prime and t an integer with $t^2 \equiv 1 \pmod{p}$, and suppose that p is not a divisor of $t - 1$. Then $\gcd(p, t - 1) \neq p$, since $\gcd(p, t - 1)$ is a divisor of $t - 1$. Since the only divisors of p are p and 1, and since $\gcd(p, t - 1)$ is a divisor of p, it follows that $\gcd(p, t - 1) = 1$. Now since $p|(t^2 - 1) = (t - 1)(t + 1)$ and $\gcd(p, t - 1) = 1$ it follows from Part (*ii*) above that $p|(t + 1)$. So either $p|(t - 1)$, which gives $t \equiv 1 \pmod{p}$, or $p|(t + 1)$, which gives $t \equiv -1 \pmod{p}$, as required.

4. (*i*) A user of the RSA cryptosystem has chosen $(2329127, 331)$ as the public key. Given that 2063 is a factor of 2329127, determine the private key.

(*ii*) Suppose that you are user of the Elgamal cryptosystem and that your public key is $(p, b, k) = (43, 3, 41)$ and your private key is $m = 6$.

(a) Check that the necessary relationship between the private key and the public key is satisfied.

(b) You receive the message $\langle 2, [1, 20, 21]\rangle$. Decrypt it.

(*iii*) Let $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and let a_1, a_2, a_3, ... be an infinite sequence of elements of S such that a_{i+1} is determined by a_i for every i. (That is, $a_{i+1} = f(a_i)$ for some function f from S to S.) Show that there exists a positive integer k such that $a_{2k} = a_k$.

Solution: (*i*) In the RSA cryptosystem the public key aways has the form (n, e) where n is the product of two distinct primes and e is coprime to $\phi(n)$. Moreover, the private key is then (n, d), where d is the inverse of e modulo $\phi(n)$. Since we are given that $n = 2329127$ and 2063 is a divisor of

2329127 we conclude that 2063 and $2329127/2063 = 1129$ are both prime, and so $\phi(n) = 2062 \times 1128 = 2325936$. Applying the extended Euclidean Algorithm to find the inverse of 331 modulo 2325936 yields the following table.

2325936	331	330	1	0
		7026	1	330
0	1	7026^-	7027	
1	0	1	1^-	

We conclude that $331 \times 7027 - 1 \times 2325936 = 1$, and so the inverse of 331 modulo $\phi(n)$ is 7027. So the private key must be $(2329127, 7027)$.

(*ii*) (a) The required relationship is that b^m computed in residue arithmetic modulo p must equal k. Noting that 86 is a multiple of 43, we find that modulo 43

$$3^6 = 3^2 \times 3^4 = 9 \times 81 \equiv 9 \times -5 = -45 \equiv 41$$

as required.

(b) The scrambling factor is the first component of the ciphertext raised to the power m, computed in residue arithmetic modulo p. So in this case it is the residue modulo 43 of $2^6 = 64$. That is, the scrambling factor is 21. Observe that $2 \times 21 = -1$ in residue arithmetic modulo 43; so $21^{-1} = -2 = 41$ (in residue arithmetic modulo 43). Hence the deciphered message is

$$\begin{aligned}[1 \times 21^{-1}, 20 \times 21^{-1}, 21 \times 21^{-1}] &= [41, 20 \times -2, 1] \\ &= [41, -40, 1] \\ &= [41, 3, 1]\end{aligned}$$

(*iii*) Since $a_1, a_2, \ldots, a_{11}$ all lie in the set S, and S has only 10 distinct elements, there must exist integers i and j with $1 \leq i < j \leq 11$ and $a_i = a_j$. We now use induction on m to show that $a_{i+m} = a_{j+m}$ for all integers $m \geq 0$. When $m = 0$ the statement is $a_i = a_j$, which we already know to be true, and this starts the induction. Now if $a_{i+m} = a_{j+m}$ for some nonnegative integer m then

$$a_{i+m+1} = f(a_{i+m}) = f(a_{j+m}) = a_{j+m+1},$$

which shows that if the statement is true for m then it is also true for $m + 1$, completing the induction.

Put $n = j - i$, noting that $n > 0$ since $j > i$. The statement that $a_{i+m} = a_{j+m}$ for all $m \geq 0$ can be restated as $a_{i+m} = a_{(i+n)+m}$ for all

$m \geq 0$, or $a_h = a_{h+n}$ for all $h \geq i$ (writing h for $i+m$). We proceed to show that $a_r = a_{r+qn}$ for all integers $q \geq 0$ and $r \geq i$, using induction on q. The case $q = 0$ is obvious and starts the induction. Now suppose that q is a nonnegative integer such that $a_r = a_{r+qn}$ for all integers $r \geq i$. If $r \geq i$ then certainly $r + qn \geq i$, since q and n are nonnegative, and since $a_h = a_{h+n}$ for all $h \geq i$ it follows that $a_{r+qn} = a_{r+qn+n} = a_{r+(q+1)n}$ for all $r \geq i$. Hence $a_r = a_{r+(q+1)n}$ for all $r \geq i$, as required to complete our induction.

Choose any integer s with $s \geq i/n$. Then $sn \geq i$ (since $n > 0$), and so $a_{sn} = a_{sn+qn}$ for all $q \geq 0$ (putting $r = sn$ in the statement just proved). In particular this holds for $q = s$, and so $a_k = a_{2k}$ holds with $k = sn$.

5. (*i*) Let p be an odd prime and $n \equiv -1 \pmod{p}$. Let q be prime divisor of $N = \sum_{i=0}^{p-1} n^{ip} = 1 + n^p + n^{2p} + \cdots + n^{(p-1)p}$. Find $\mathrm{ord}_q(n)$, and then show that $q \equiv 1 \pmod{p^2}$.

(*ii*) Let p be an odd prime.

(a) Show that if k is a positive integer then $p^k \equiv 3 \pmod 4$ if and only if $p \equiv 3 \pmod 4$ and k is odd.

(b) Let ℓ be a positive integer and let s be the sum of the positive divisors of p^ℓ. Show that s is odd if and only if ℓ is even.

(c) Again let ℓ be a positive integer and s be the sum of the positive divisors of p^ℓ. Show that $s \equiv 2 \pmod 4$ if and only if and $p \equiv 1 \pmod 4$ and $\ell \equiv 1 \pmod 4$.

(*iii*) Using Part (*ii*), show that if n is an odd perfect number then $n = p^\ell m^2$ for some integers p, ℓ and m such that p is prime and $p \equiv \ell \equiv 1 \pmod 4$.

Solution: (*i*) Since $\sum_{i=0}^{p-1} n^{ip}$ is a geometric series with common ratio n^p, with p terms and with 1 as the first term, the geometric series formula gives

$$N = ((n^p)^p - 1)/(n^p - 1) = (n^{p^2} - 1)/(n^p - 1).$$

Since q is a divisor of N it is a divisor of $(n^p - 1)N = n^{p^2} - 1$; that is, $n^{p^2} \equiv 1 \pmod q$. So $\mathrm{ord}_q(n)$ is a divisor of p^2.

Suppose, for a contradiction, that $\mathrm{ord}_q(n)$ is a divisor of p. This implies that $n^p \equiv 1 \pmod q$. So

$$N = \sum_{i=0}^{p-1} (n^p)^i \equiv \sum_{i=0}^{p-1} 1^i \equiv p \pmod q,$$

and since q is a divisor of N it follows that $p \equiv 0 \pmod{q}$. Since p and q are both primes this forces $q = p$, and since we are given that $n \equiv -1 \pmod{p}$ it follows that $n \equiv -1 \pmod{q}$. And so $n^p \equiv (-1)^p \equiv -1 \pmod{q}$, since p is odd. This gives our desired contradiction, since $n^p \equiv 1 \pmod{q}$ and certainly $1 \not\equiv -1 \pmod{q}$ (since 2 is not divisible by the odd prime q).

We conclude that $\mathrm{ord}_q(n)$ is a divisor of p^2 that is not a divisor of p, and since p is a prime the only such number is p^2 itself. So $\mathrm{ord}_q(n) = p^2$.

If n were a multiple of q then we would have $n^{p^2} \equiv 0 \pmod{q}$, contrary to the fact that $n^{p^2} \equiv 1 \pmod{q}$. So n is not a multiple of q, and Fermat's Little Theorem tells us that $n^{q-1} \equiv 1 \pmod{q}$. Hence $\mathrm{ord}_q(n)$ is a divisor of $q - 1$. Thus $p^2 | (q-1)$, and so $q \equiv 1 \pmod{p^2}$.

(*ii*) (a) Since p is odd the remainder when p is divided by 4 must be either 1 or 3. So either $p \equiv 1 \pmod{4}$ or $p \equiv 3 \equiv -1 \pmod{4}$. In the former case, if k is any positive integer then $p^k \equiv 1^k \equiv 1 \not\equiv -1 \pmod{p}$ (since p is not a divisor of 2). In the latter case

$$p^k \equiv (-1)^k \equiv \begin{cases} +1 \pmod{p} & \text{if } k \text{ is even,} \\ -1 \pmod{p} & \text{if } k \text{ is odd.} \end{cases}$$

Thus, since $-1 \equiv 3 \pmod{4}$, we have shown that if $p \equiv 3 \pmod{4}$ and k is odd then $p^k \equiv 3 \pmod{4}$, and in all other cases $p^k \not\equiv 3 \pmod{4}$, as required.

(b) The positive divisors of p^ℓ are the integers p^i for $i \in \{0, 1, 2, \ldots, p^\ell\}$. Thus

$$s = 1 + p + p^2 + \cdots + p^\ell = \sum_{i=0}^{\ell} p^i.$$

Since p is odd, $p \equiv 1 \pmod{2}$. So $s \equiv \sum_{i=0}^{\ell} 1^i \pmod{2}$; that is, $s \equiv \ell + 1 \pmod{2}$. So s is even if and only if ℓ is odd, as required.

(c) Suppose first that $p \equiv -1 \pmod{4}$. Then

$$s = 1 + p + p^2 + \cdots + p^\ell \equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^\ell \pmod{4}$$

and if ℓ is odd the right hand side is zero, since the total number of terms is even and every second term cancels the term that precedes it. On the other hand, if ℓ is even then the last term on the right hand side is 1, and the preceding ℓ terms cancel out in pairs, leaving 1 as the value of the right hand side. So if $p \equiv -1 \pmod{4}$ then s is congruent mod 4 to either 0 or 1, but never congruent to 2.

On the other hand, if $p \equiv 1 \pmod{4}$ then $p^i \equiv 1 \pmod{4}$ for all i, and so $s = \sum_{i=0}^{\ell} p^i \equiv \sum_{i=0}^{\ell} 1 \equiv \ell + 1 \pmod{4}$, giving $s \equiv 2 \pmod{4}$ if and only if $\ell \equiv 1 \pmod{4}$, as required.

(*iii*) Suppose that n is an odd perfect number, and let $p_1, p_2, \ldots, p_k$ be the prime divisors of n. Thus

$$n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}$$

for some positive integers $\ell_1, \ell_2, \ldots, \ell_k$, and since the sum-of-divisors σ function is multiplicative,

$$\sigma(n) = \sigma(p_1^{\ell_1})\sigma(p_2^{\ell_2)} \cdots \sigma(p_k^{\ell_k}).$$

We are given that n is perfect; so by definition n equals the sum of all the proper divisors n. Hence $\sigma(n) = 2n$. Observe that since n is odd this quantity is divisible by 2 but not by 4. But $2n$ is the product of the positive integers $\sigma(p_i^{\ell_i})$, for i from 1 to k, and it follows that exactly one of these numbers are even (since if two or more were even their product would be divisible by at least 2^2, and if none were even their product would not be divisible by 2). Moreover the one that is even must be congruent to 2 mod 4, since if it were congruent to 0 mod 4 then the product would be divisible by 4.

Renumbering the factors if necessary, we may assume that $\sigma(p_1^{\ell_1})$ is congruent to 2 mod 4, and $\sigma(p_i^{\ell_i})$ is odd for all i from 2 to k. By (*ii*) (b) it follows that ℓ_i is even when $2 \le i \le k$, and so we may write $\ell_i = 2h_i$ in these cases. And by (*ii*) (c) it follows that $p_1 \equiv 1 \pmod 4$ and $\ell_1 \equiv 1 \pmod 4$. Thus

$$n = p_1^{\ell_1}(p_2^{2h_2} p_3^{2h_3} \cdots p_k^{2h_k}) = p^{\ell} m^2$$

where $m = p_2^{h_2} p_3^{h_3} \cdots p_k^{h_k}$ and $p = p_1$ is a prime congruent to 1 (mod 4) and $\ell = \ell_1$ is a positive integer congruent to 1 (mod 4), as required.

6. (MATH2988 students only)

(*i*) Let n be a positive integer. Prove that $\sum_{d|n} \phi(d) = n$.

(*ii*) Let $a_1 > a_2 > a_3 > \cdots > a_k$ be the successive remainders generated when the Euclidean Algorithm is used to determine $d = \gcd(a, b)$, where $(a_1, a_2) = (a, b)$ and $a_k = d$. Show that $k < 2\log_2(a) + 1$.

(*iii*) Let n be an integer greater than 1. Show that n is not a divisor of $2^n - 1$. (Consider $\mathrm{ord}_p(2)$ for prime divisors of n.)

Solution: (*i*) Consider the n fractions $\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$, and in each case cancel away the greatest common divisor of the numerator and the denominator, producing a fraction that is in its lowest terms. The resulting fractions

all have the form $\frac{i}{d}$ where i and d are coprime, $0 \le i < d$, and $d|n$. For each given divisor d of n the total number of possible values for i is $\phi(d)$, since this is the size of the set $\{\, i \mid 0 \le i < d \text{ and } \gcd(i,d) = 1 \,\}$, and they all occur since $\frac{i}{d} = \frac{id'}{n}$, where $dd' = n$. So the total number of fractions we end up with is $\sum_{d|n} \phi(d)$, and since we started out with n fractions we conclude that $\sum_{d|n} \phi(d) = n$, as required.

(*ii*) According to the rules that define the Euclidean algorithm, the sequence $a_0, a_1, \ldots, a_k$ is generated as follows: if $i \in \{1, 2, \ldots, k-1\}$ then a_{i+1} is the remainder obtained when a_i is divided into a_{i-1}. That is,

$$a_{i+1} = a_{i-1} - q_i a_i \tag{1}$$

where q_i is the largest integer less than or equal to a_{i-1}/a_i.

Let $i \in \{2, 3, \ldots, k-2\}$ be arbitrary; we shall show that $a_{i+2} < \frac{1}{2}a_i$. This is obviously true if $a_{i+1} \le \frac{1}{2}a_i$, since $a_{i+2} < a_{i+1}$. But if $a_{i+1} > \frac{1}{2}a_i$ then $1 < a_i/a_{i+1} < 2$, and so the quotient q_{i+1} obtained when a_i is divided by a_{i+1} is 1. Thus by (1) above, with i replaced by $i+1$,

$$a_{i+2} = a_i - a_{i+1} < a_i - \tfrac{1}{2}a_i = \tfrac{1}{2}a_i.$$

So in either case we have $a_{i+2} < \frac{1}{2}a_i$, as claimed.

It follows by induction that if ℓ is any positive integer with $1 + 2\ell \le k$ then $a_{1+2\ell} < 2^{-\ell}a_1$. When $\ell = 1$ this reduces to $a_3 < \frac{1}{2}a_1$, which is $a_{i+2} < \frac{1}{2}a_i$ in the case $i = 1$, and for the inductive step observe that if $\ell > 1$ and $a_{1+2(\ell-1)} < 2^{-(\ell-1)}a_1$ then, by $a_{i+2} < \frac{1}{2}a_i$ in the case $i = 2\ell - 1$,

$$a_{1+2\ell} < \tfrac{1}{2}a_{2\ell-1} < \tfrac{1}{2}(2^{-(\ell-1)}a_1) = 2^{-\ell}a_1,$$

as required to complete the induction. Moreover, a totally analogous induction gives $a_{2+2\ell} < 2^{-\ell}a_2$ for each positive integer ℓ with $2 + 2\ell \le k$.

If $k = 1 + 2\ell$ is odd then by the previous paragraph we have that $a_k < 2^{-\ell}a_1$, and so

$$2^\ell \le 2^\ell a_k < a_1,$$

whence $\ell < \log_2 a_1 = \log_2 a$ and $k = 2\ell + 1 < 2\log_2 a + 2$. If $k = 2\ell$ is even then the previous paragraph gives $a_k < 2^{-(\ell-1)}a_2 < 2^{-(\ell-1)}a$, and so

$$2^{(\ell-1)} \le 2^{(\ell-1)}a_k < a,$$

whence $\ell - 1 < \log_2 a$ and $k = 2\ell < 2\log_2 a + 2$. So in either case $k = 2\log_2 a + 2$.

(*iii*) Suppose that $n > 1$ is a divisor of $2^n - 1$. By the Fundamental Theorem of Arithmetic, n has at least one prime divisor. Choose p to be the least

prime divisor of n. Since $p|n$ and $n|(2^n - 1)$ it follows that $p|(2^n - 1)$, and so $2^n \equiv 1 \pmod{p}$. Hence $\text{ord}_p(2)$ is a divisor of n. Obviously 2 is not a multiple of p (since $2^n \not\equiv 0 \pmod{p}$); so Fermat's Little Theorem gives $2^{p-1} \equiv 1 \pmod{p}$, and hence $\text{ord}_p(2) \leq p - 1$. So we have shown that $\text{ord}_p(2)$ is a divisor of n that is less than the smallest prime divisor of n. So $\text{ord}_p(2) = 1$, which is absurd since $2^1 \not\equiv 1 \pmod{p}$. So if $n > 1$ then assuming also that $n|(2^n - 1)$ leads to a contradiction. So n is not a divisor of $2^n - 1$.