

### Assignment 2

1. (i) It is well known that if a positive integer  $n$  is expressed in the usual base 10 notation, then  $n$  is divisible by 9 if and only if the sum of its decimal digits is a multiple of 9. Prove this result. [Hint: Consider  $n - s$ , where  $s$  is the sum of the digits.]
- (ii) Let  $n = (123456713572461473625152637416427531765432)_8$  (expressed in octal notation.) Is  $n$  a multiple of 7?

*Solution.*

- (i) Let  $n = (a_k a_{k-1} \dots a_0)_{10}$ . That is,  $a_k, a_{k-1}, \dots, a_0$  are the base 10 (or decimal) digits of  $n$ . Then

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_0$$

and the sum of the decimal digits of  $n$  is

$$s = a_k + a_{k-1} + \dots + a_0.$$

Since  $10 \equiv 1 \pmod{9}$  and multiplication respects congruences it follows that  $10^i \equiv 1^i \equiv 1 \pmod{9}$ , and since addition also respects congruences it follows that

$$n \equiv \sum_{i=0}^k a_i 10^i \equiv \sum_{i=0}^k a_i \equiv s \pmod{9}.$$

So if  $n \equiv 0 \pmod{9}$  then  $s \equiv 0 \pmod{9}$ , and if  $s \equiv 0 \pmod{9}$  then  $n \equiv 0 \pmod{9}$ . That is,  $n$  is a multiple of 9 if and only if  $s$  is a multiple of 9, as required.

- (ii) Since  $8 \equiv 1 \pmod{7}$  it follows that  $8^i \equiv 1 \pmod{7}$  for all natural numbers  $i$ , and so  $\sum_i a_i 8^i \equiv 0 \pmod{7}$  if and only if  $\sum_i a_i \equiv 0 \pmod{7}$ . So if an integer  $n$  is expressed in octal notation and the sum of the octal digits is a multiple of 7 then  $n$  will also be a multiple of 7. In the present example we see that the octal representation of  $n$  has six 1's, six 2's, six 3's, six 4's, six 5's, six 6's and six 7's (and no 0's), and so the sum of the octal digits is  $6 \times (1 + 2 + 3 + 4 + 5 + 6 + 7) = 6 \times 28$ , a multiple of 7. So  $n$  is a multiple of 7.

2. Find the smallest integer  $n$  such that  $\phi(n) < 0.192n$  (where  $\phi$  is Euler's phi function). To obtain full marks you must show that your answer is correct.

*Solution.*

Suppose that  $n$  is the smallest positive integer such that  $\phi(n)/n < 0.192$ , and let  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ , where the  $p_i$  are pairwise distinct prime numbers and the  $k_i$  are positive integers. By the formula for  $\phi(n)$  proved in lectures,

$$\frac{\phi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Notice that this expression does not depend on the exponents  $k_i$ , and if any one of these exponents is greater than 1 then

$$p_1 p_2 \dots p_r < p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

So if we define  $n' = p_1 p_2 \dots p_r$  then  $\phi(n')/n' = \phi(n)/n$  and  $n' < n$ , contradicting our assumption that  $n$  is the smallest positive integer with  $\phi(n)/n < 0.192$ . So all the  $k_i$  are equal to 1.

We may choose the numbering of the primes  $p_i$  appearing in the factorization of  $n$  so that  $p_1 < p_2 < \dots < p_r$ ; in particular,  $p_r$  is the largest of them. We shall prove that  $p_1, p_2, \dots, p_{r-1}$  are all the prime numbers less than  $p_r$ : every prime number less than the largest prime factor of  $n$  is also a prime factor of  $n$ . So suppose, for a contradiction, that there is some prime  $q < p_r$  that does not appear in the set  $\{p_1, p_2, \dots, p_{r-1}\}$ . Let  $m = p_1 p_2 \dots p_{r-1} q$ . That is, the prime factorization of  $m$  is the same as the prime factorization of  $n$ , except that  $p_r$  has been replaced by  $q$ . So  $m = n(q/p_r) < n$ , since  $q < p_r$ . Moreover, since  $q < p_r$  it follows that  $\frac{1}{q} > \frac{1}{p_r}$ , and so  $1 - \frac{1}{q} < 1 - \frac{1}{p_r}$ . Hence

$$\begin{aligned} \frac{\phi(m)}{m} &= \left( \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_{r-1}}\right) \right) \left(1 - \frac{1}{q}\right) \\ &< \left( \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_{r-1}}\right) \right) \left(1 - \frac{1}{p_r}\right) \\ &= \frac{\phi(n)}{n} < 0.192 \end{aligned}$$

contradicting the fact that  $n$  is the smallest positive integer with  $\phi(n)/n < 0.192$ .

We have now shown that the prime factors of  $n$  are precisely all the prime numbers up to  $p_r$ . That is,  $n$  has the form  $n = p_1 p_2 \dots p_r$ , where  $p_1$  is the smallest prime integer (namely 2),  $p_2$  is the next smallest (namely 3),  $p_3$  the next smallest (namely 5), and so on. Clearly the larger  $r$  is, the larger  $n$  is: it is just a question of how far we have to go to make  $\prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) < 0.192$ . Trying

successively  $r = 1$ , then  $r = 2$ , then  $r = 3$ , and so on, we find the following values for  $\prod_{i=1}^r (1 - \frac{1}{p_i})$ .

$$\begin{aligned} & \frac{1}{2}, \\ & \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}, \\ & \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = \frac{1}{3} \cdot \frac{4}{5} = \frac{4}{15}, \\ & \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = \frac{4}{15} \cdot \frac{6}{7} = \frac{8}{35}, \\ & \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} = \frac{8}{35} \cdot \frac{10}{11} = \frac{16}{77}, \\ & \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} = \frac{16}{77} \cdot \frac{12}{13} = \frac{192}{1001}. \end{aligned}$$

Since  $\frac{192}{1001} < 0.192$ , the answer is  $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$ .

- \*3. (MATH2988) A positive integer  $n$  is called a *Sierpinski number* if  $2^k n + 1$  is composite for all natural numbers  $k$ . The smallest  $n$  definitely known to be a Sierpinski number is 78557. Prove that for each natural number  $k$  there exists  $p \in \{3, 5, 7, 13, 19, 37, 73\}$  such that  $p$  is a factor of  $2^k \times 78557 + 1$ .

*Solution.*

Let us start by attempting to discover which natural numbers  $k$  have the property that  $2^k \times 78557 + 1$  is divisible by 73. Note first that  $78557 \equiv 9 \pmod{73}$ ; so  $2^k \times 78557 + 1 \equiv 0 \pmod{73}$  if and only if  $2^k \times 9 \equiv -1 \pmod{73}$ . Multiplying both sides by 8 and using  $9 \times 8 = 72 \equiv -1 \pmod{73}$ , we find that  $2^k \times 78557 + 1$  is divisible by 73 if and only if  $2^k \equiv 8 \pmod{73}$ .

Let  $m = \text{ord}_{73}(2)$ , the smallest positive integer such that  $2^m \equiv 1 \pmod{73}$ . We know from lectures that  $2^k \equiv 2^h \pmod{73}$  if and only if  $k \equiv h \pmod{m}$ , and since obviously  $2^3 \equiv 8 \pmod{73}$  we conclude that  $2^k \equiv 8 \pmod{73}$  if and only if  $k \equiv 3 \pmod{m}$ .

To determine  $m$ , first recall (from Fermat's Little Theorem) that  $m$  must be a divisor of 72. If  $1 \leq i \leq 6$  then  $2 \leq 2^i \leq 64$ , and so  $2^i \not\equiv 1 \pmod{73}$ . The next divisor of 72 to check is 8, and we see that  $2^8 = 256 \equiv 37 \not\equiv 1 \pmod{73}$ . The next one is 9, and indeed  $2^9 = 512 = 7 \times 73 + 1$ . So  $m = 9$ , and we have shown that  $2^k \times 78557 + 1$  is divisible by 73 if and only if  $k \equiv 3 \pmod{9}$ .

We proceed to apply the same strategy for all the other primes in the set  $\{3, 5, 7, 13, 19, 37, 73\}$ .

Since  $78557 \equiv 6 \pmod{37}$  we see that  $2^k \times 78557 + 1$  is divisible by 37 if and only if  $2^k \times 6 \equiv -1 \pmod{37}$ , which in turn is equivalent to  $2^k \equiv 6 \pmod{37}$ . Now  $2^6 = 64 \equiv -10 \pmod{37}$ , and so  $2^{12} \equiv 100 \equiv -11 \pmod{37}$

and  $2^{18} \equiv 2^6 \times 2^{12} \equiv 110 \equiv -1$ . So  $\text{ord}_{37}(2)$  is a divisor of 36 that is not a divisor of 18 or 12; so it must be 36. (That is, 2 is a primitive root mod 37.) Moreover, since  $2^9 \equiv 2^6 \times 2^3 \equiv -80 \equiv -6$  and  $2^{18} \equiv -1$ , we see that  $2^{27} \equiv 6$ . So  $2^k \times 78557 + 1$  is divisible by 37 if and only if  $k \equiv 27 \pmod{36}$ .

Since  $78557 \equiv 11 \pmod{19}$  we see that  $2^k \times 78557 + 1$  is divisible by 19 if and only if  $2^k \times 11 \equiv -1 \pmod{19}$ , which in turn is equivalent to  $2^k \equiv 12 \pmod{19}$ . Now  $2^6 = 64 \equiv 7 \pmod{19}$  and  $2^9 = 2^6 \times 2^3 \equiv 7 \times 8 \equiv -1 \pmod{19}$ . So  $\text{ord}_{19}(2)$  is a divisor of 18 that is not a divisor of 6 or 9, and we deduce that 2 is a primitive root mod 19. Now  $2^4 \equiv -3 \pmod{19}$ ; so  $2^4 \times 2^2 \times 2^9 \equiv (-3) \times 4 \times (-1) \pmod{19}$ , and we deduce that  $2^k \times 78557 + 1$  is divisible by 19 if and only if  $k \equiv 15 \pmod{18}$ .

Since  $78557 \equiv 11 \pmod{13}$  we see that  $2^k \times 78557 + 1$  is divisible by 13 if and only if  $2^k \times 11 \equiv -1 \pmod{13}$ , which is equivalent to  $2^k \equiv 7 \pmod{13}$ . Now  $2^6 = 64 \equiv -1 \pmod{13}$  and  $2^4 \equiv 3 \pmod{13}$ ; so 2 is a primitive root mod 13. We have  $2^4 \equiv 3 \pmod{13}$ ; so  $2^4 \times 2^6 \equiv -3$  and  $2^{11} \equiv -6 \equiv 7$ . So  $2^k \times 78557 + 1$  is divisible by 13 if and only if  $k \equiv 11 \pmod{12}$ .

Observe that  $78557 \equiv 3 \pmod{7}$  and  $\text{ord}_7(2) = 3$ . So  $2^k \times 78557 + 1 \equiv 2^k \times 3 + 1$  is divisible by 7 if and only if  $k \equiv 1 \pmod{3}$ .

Clearly  $2^k \times 78557 + 1 \equiv 2^k \times 2 + 1 \pmod{5}$ , and since 2 is a primitive root mod 5 we deduce that  $2^k \times 78557 + 1$  is divisible by 5 if and only if  $k \equiv 1 \pmod{4}$ .

Finally, since  $\text{ord}_3(2) = 2$  we see that  $2^k \times 78557 + 1 \equiv 2^k \times 2 + 1$  is divisible by 3 if and only if  $k$  is even.

Now let  $k$  be an arbitrary natural number. If the residue of  $k \pmod{36}$  is even then  $k$  itself is even, and so  $2^k \times 78557 + 1$  is divisible by 3. If the residue of  $k \pmod{36}$  is odd then either  $k \equiv 1 \pmod{4}$ , in which case  $2^k \times 78557 + 1$  is divisible by 5, or else the residue of  $k \pmod{36}$  is one of the numbers 3, 7, 11, 15, 19, 23, 27, 31 or 35. If the residue is 7, 19 or 31 then  $k \equiv 1 \pmod{3}$ , and  $2^k \times 78557 + 1$  is divisible by 7. If the residue is 11, 23 or 35 then  $k \equiv 11 \pmod{12}$ , and  $2^k \times 78557 + 1$  is divisible by 13. The remaining residues are 3, 15 and 27. The first of these gives  $k \equiv 3 \pmod{9}$ , making  $2^k \times 78557 + 1$  divisible by 73, the next gives  $k \equiv 15 \pmod{18}$ , making  $2^k \times 78557 + 1$  divisible by 19, and in the remaining case, namely  $k \equiv 27 \pmod{36}$ ,  $2^k \times 78557 + 1$  is divisible by 37.