Elementary Number Theory - Exercise 4a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Show that if m is composite, then $2^m - 1$ is composite.
Hint: If $m = ab$, show that $2^a - 1 \mid 2^m - 1$.

Solution 1. By the geometric sum formula, we have $\frac{2^{ab}-1}{2^a-1} = \sum_{j=0}^{b-1} 2^{aj}$, which is an integer. If $a, b > 1$, then both $\frac{2^{ab}-1}{2^a-1}$ and $2^a - 1$ are bigger than 1, so $2^m - 1$ is composite.

Problem 2. Show that a natural number of the form $n = 2^{m-1}(2^m - 1)$, with $2^m - 1$ being prime, is perfect.

Solution 2. We need to show that $\sigma(n) = 2n$. Since σ is multiplicative, we have

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1).$$

In an earlier exercise, we have shown the formula

$$\sigma(2^{m-1}) = \frac{2^m - 1}{2 - 1} = 2^m - 1.$$

Moreover, for primes p we have $\sigma(p) = p + 1$, so for the prime $2^m - 1$ we get

$$\sigma(2^m - 1) = 2^m.$$

In total, we get

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1) \cdot 2^m = 2n,$$

so n is perfect.

Problem 3. Check that 6 and 28 are perfect, and find the next two even perfect numbers.

Solution 3. We have $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$ and $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28$. By Euler's criterion from the lecture, the even perfect numbers are precisely those of the form $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ prime (hence p must be prime by the first problem). We list some values:

$$\begin{aligned}
p = 2 : &\quad n = 2 \cdot 3 = 6, \\
p = 3 : &\quad n = 4 \cdot 7 = 28, \\
p = 5 : &\quad n = 16 \cdot 31 = 496, \\
p = 7 : &\quad n = 64 \cdot 127 = 8128, \\
p = 11 : &\quad \text{In this case } 2^p - 1 = 2047 = 23 \cdot 89 \text{ is not prime!} \\
p = 13 : &\quad n = 4096 \cdot 8191 = 33550336.
\end{aligned}$$

Problem 4. Show that every even perfect number ends with the digit 6 or 8.

Solution 4. We use that every even perfect number is of the form $n = 2^{p-1}(2^p - 1)$ for a prime p, and reduce modulo 10. We will frequently use that any non-zero power of a number that ends with a 6, also ends with a 6 (compute modulo 10 to see this).

For $p = 2$ we have $n = 6$, which indeed ends with 6.

If p is an odd prime, then p is of the form $p = 4k + 1$ or $p = 4k + 3$ for some $k \in \mathbb{N}$. If $p = 4k + 1$, then we compute modulo 10 to see that

$$n \equiv 2^{4k}(2^{4k+1} - 1) \equiv 16^k(2 \cdot 16^k - 1) \equiv 6 \cdot (2 \cdot 6 - 1) \equiv 6 \cdot 11 \equiv 6 \pmod{10},$$

so n ends with the digit 6.

If $p = 4k + 3$ then

$$\begin{aligned} n &\equiv 2^{4k+2}(2^{4k+3} - 1) \equiv 4 \cdot 16^k \cdot (8 \cdot 16^k - 1) \equiv 4 \cdot 6 \cdot (8 \cdot 6 - 1) \\ &\equiv 24 \cdot 47 \equiv 4 \cdot 7 \equiv 28 \equiv 8 \pmod{10}, \end{aligned}$$

so n ends with 8.

Problem 5. Show that every even perfect number n can be written as the sum of the first d natural numbers, $n = 1 + 2 + 3 + \ldots + d$, for a suitable $d \in \mathbb{N}$.

Solution 5. By Euler's criterion, we have $n = 2^{m-1}(2^m - 1)$ for some m. On the other hand, we have the well-known summation formula

$$1 + 2 + \ldots + d = \frac{(d+1)d}{2}$$

for any natural number d. For $d = 2^m - 1$ we obtain

$$1 + 2 + \ldots + (2^m - 1) = \frac{2^m(2^m - 1)}{2} = 2^{m-1}(2^m - 1) = n.$$

Problem 6. We have seen that an *odd* perfect number must be of the form $n = p^{2m+1}Q^2$ with an odd prime p and an odd natural number Q with $\gcd(p, Q) = 1$.

Show that p must be of the form $p = 4k + 1$, and m must be even.
Hint: Use that $\sigma(p^{2m+1}) = (1 + p)(1 + p^2 + p^4 + \cdots + p^{2m})$.

Solution 6. Since $2n = \sigma(n) = \sigma(p^{2m+1})\sigma(Q^2)$ and $\sigma(p^{2m+1}) = (1+p)(1+p^2+p^4+\ldots p^{2m})$, we see that $(1 + p)$ divides $2n$. If p would be of the form $p = 4k + 3$, then $1 + p = 4k + 4$ would be divisible by 4, but $2n$ is only divisible by 2. Hence p must be of the form $4k + 1$.

Since $(1 + p)(1 + p^2 + p^4 + \cdots + p^{2m})$ divides $2n$, since $1 + p$ is already even, the sum $1 + p^2 + p^4 + \cdots + p^{2m}$ divides n and hence must be odd. Since $1 + p^2 + p^4 + \cdots + p^{2m}$ is a sum of $m + 1$ odd numbers, it is odd if and only if m is even.

Problem 7. (Homework) Prove Thabit's rule and apply it to $k \in \{1, \ldots, 10\}$ to find three pairs of amicable numbers[1].

[1] Until today, only these three pairs of amicable numbers satisfying Tabit's rule have been found.

Solution 7. Suppose that

$$T_k = 3 \cdot 2^k - 1,$$
$$T_{k-1} = 3 \cdot 2^{k-1} - 1,$$
$$R_k = 9 \cdot 2^{2k-1} - 1$$

are all prime. Then Thabit's rule says that the number

$$m = 2^k T_k T_{k-1} \quad n = 2^k R_k$$

form an amicable pair. We have to show tht $\sigma(m) = \sigma(n) = m + n$. Using that σ is multiplicative, and the formulas $\sigma(2^k) = \frac{2^{k+1}-1}{2-1} = 2^{k+1} - 1$ and $\sigma(p) = p + 1$ for primes p, we compute

$$\sigma(m) = \sigma(2^k T_k T_{k-1}) = (2^{k+1}-1)(T_k+1)(T_{k-1}+1) = (2^{k+1}-1) \cdot 3 \cdot 2^k \cdot 3 \cdot 2^{k-1} = (2^{k+1}-1) \cdot 9 \cdot 2^{2k-1}$$

and

$$\sigma(n) = \sigma(2^k R_k) = (2^{k+1} - 1)(R_k + 1) = (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}.$$

Finally, we have

$$\begin{aligned} m + n &= 2^k T_k T_{k-1} + 2^k R_k = 2^k \cdot ((3 \cdot 2^k - 1)(3 \cdot 2^{k-1} - 1) + 9 \cdot 2^{2k-1} - 1) \\ &= 2^k \cdot (9 \cdot 2^{2k-1} - 3 \cdot 2^k - 3 \cdot 2^{k-1} + 1 + 9 \cdot 2^{2k-1} - 1) \\ &= (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1} = \sigma(m) = \sigma(n), \end{aligned}$$

so m and n are amicable.

If we list the numbers $T_k = 3 \cdot 2^k - 1, T_{k-1}$, and $R_k = 9 \cdot 2^{2k-1} - 1$ for $k \in \{1, \dots, 10\}$, we see that they are all prime only for $k \in \{2, 4, 7\}$. In these cases we compute

$$\begin{aligned} &2^2 T_2 T_1 = 220, \quad 2^2 R_2 = 284, \\ &2^4 T_4 T_3 = 17296, \quad 2^4 R_4 = 18416, \\ &2^7 T_7 T_6 = 9363584, \quad 2^7 R_7 = 9437056. \end{aligned}$$

Hence, we get the amicable pairs

$$(220, 284), \quad (17296, 18416), \quad (9363584, 9437056).$$

Problem 8 (Homework)**.** The *harmonic mean* of the divisors of a natural number n is defined by

$$H(n) = \frac{n\tau(n)}{\sigma(n)}.$$

For example, $H(4) = \frac{4\tau(4)}{\sigma(4)} = \frac{4 \cdot 3}{7} = \frac{12}{7}$. A number n is called *harmonic* if the harmonic mean $H(n)$ of its divisors is an integer.

1. Check that 6 and 140 are harmonic numbers.

2. Show that every perfect number is harmonic.

Solution 8. We have

$$H(6) = \frac{6\tau(6)}{\sigma(6)} = \frac{6 \cdot (1+1+1+1)}{(1+2+3+6)} = \frac{6 \cdot 4}{12} = 2,$$

and

$$H(140) = \frac{140\tau(140)}{\sigma(140)} = \frac{140\tau(4 \cdot 5 \cdot 7)}{\sigma(4 \cdot 5 \cdot 7)} = \frac{140 \cdot 3 \cdot 2 \cdot 2}{7 \cdot 6 \cdot 8} = \frac{140 \cdot 12}{336} = 5.$$

If n is a perfect number, then $\sigma(n) = 2n$, so the harmonic mean of its divisors is given by

$$H(n) = \frac{\tau(n)}{2}.$$

Hence it remains to show that $\tau(n)$, the number of divisors of n, is even. We have that $\tau(n)$ is odd if and only if n is a square: to see this, note that the divisors of n come in pairs $(d, n/d)$, and we have $d = n/d$ if and only if $n = d^2$ is a square. Hence we need to check that a perfect number can never be a square. If n is an even perfect number, it is of the form $n = 2^{m-1}(2^m - 1)$ with $2^m - 1$ being an odd prime, so n is not a square. If n is an odd perfect number, it is of the form $n = p^{2m+1}Q^2$ for some odd prime p and some odd natural number Q, so it is also not a square. In any case, a perfect number is not a square, so $\tau(n)$ is even, hence $H(n)$ is an integer and n is a harmonic number.

Problem 9 (sage)**.** Write programs that find

1. Mersenne primes,
2. perfect numbers,
3. pairs of amicable numbers.
   Bonus: Find some pairs that are not covered by Thabit's rule.