The University of Sydney
School of Mathematics and Statistics

Solutions to Tutorial 5 (Week 6)

MATH2068/2988: Number Theory and Cryptography Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

Recall from lectures the following multiplicative functions of a positive integer n:

$$\begin{aligned}\phi(n) &= \text{the number of nonnegative integers } a < n \text{ such that } \gcd(a,n) = 1,\\ \tau(n) &= \text{the number of positive integer divisors of } n,\\ \sigma(n) &= \text{the sum of the positive integer divisors of } n.\end{aligned}$$

If n has prime factorization $p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ with $p_1, p_2, \cdots, p_r$ being distinct primes, then

$$\begin{aligned}\phi(n) &= p_1^{k_1-1}(p_1-1)\,p_2^{k_2-1}(p_2-1)\,\cdots\,p_r^{k_r-1}(p_r-1),\\ \tau(n) &= (k_1+1)(k_2+1)\cdots(k_r+1),\\ \sigma(n) &= \frac{p_1^{k_1+1}-1}{p_1-1}\,\frac{p_2^{k_2+1}-1}{p_2-1}\,\cdots\,\frac{p_r^{k_r+1}-1}{p_r-1}.\end{aligned}$$

Tutorial Exercises:

1. Calculate $\phi(n)$, $\sigma(n)$ and $\tau(n)$ for each of $n = 27, 28, 29, 30$.

Solution: 27 has prime factorization 3^3, so

$$\phi(27) = 3^2(3-1) = 18, \quad \tau(27) = 3+1 = 4, \quad \sigma(27) = \frac{3^4-1}{3-1} = 40.$$

28 has prime factorization $2^2\,7$, so

$$\begin{aligned}&\phi(28) = 2^1(2-1)7^0(7-1) = 12, \quad \tau(28) = (2+1)(1+1) = 6,\\ &\sigma(28) = \frac{2^3-1}{2-1}\,\frac{7^2-1}{7-1} = 56 \quad \text{(which means that 28 is perfect).}\end{aligned}$$

29 is itself prime, so

$$\phi(29) = 28, \quad \tau(29) = 2, \quad \sigma(29) = 30.$$

30 has prime factorization $2^1\,3^1\,5^1$, so

$$\begin{aligned}&\phi(30) = (2-1)(3-1)(5-1) = 8, \quad \tau(30) = (1+1)(1+1)(1+1) = 8,\\ &\sigma(30) = \frac{2^2-1}{2-1}\,\frac{3^2-1}{3-1}\,\frac{5^2-1}{5-1} = 72.\end{aligned}$$

2. What is the smallest positive integer n such that $\tau(n) = 6$?

Solution: Suppose n has prime factorization $p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ and satisfies $\tau(n) = 6$. Each exponent k_i here can be assumed to be positive (otherwise we could just leave

out that factor). Thus $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$ is a product of r numbers which are all ≥ 2. There are only two ways to write 6 as a product of such numbers (not taking order into account): $6 = 6$ or $6 = 3 \times 2$. So we have either $r = 1$ and $n = p_1^5$, or $r = 2$ and $n = p_1^2 p_2$; conversely, any number n of one of these two forms satisfies $\tau(n) = 6$. The smallest number of the form p_1^5 is $2^5 = 32$; the smallest number of the form $p_1^2 p_2$ is $2^2\,3 = 12$. So the answer is 12.

3. Recall that a positive integer n is said to be *perfect* if $\sigma(n) = 2n$ (in other words, n equals the sum of all proper positive divisors of n). Even perfect numbers were discussed in lectures; it is not known whether odd perfect numbers exist.

(a) Show that a power of a prime number cannot be perfect.

Solution: If $n = p^k$ where p is prime, then $\sigma(n) = \frac{p^{k+1}-1}{p-1}$. Assume for a contradiction that $\sigma(n) = 2n$. Then

$$p^{k+1} - 1 = 2p^k(p-1) = 2p^{k+1} - 2p^k,$$

which rearranges to $p^{k+1} = 2p^k - 1$. But this implies that $p^{k+1} < 2p^k$, which implies (after dividing both sides by p^k) that $p < 2$. This is a contradiction.

(b) Show that a number of the form $3^a\,5^b$ (for some nonnegative integers a, b) cannot be perfect.

Solution: If $n = 3^a\,5^b$, then $\sigma(n) = \frac{3^{a+1}-1}{2}\,\frac{5^{b+1}-1}{4}$. Assume for a contradiction that $\sigma(n) = 2n$. Then

$$(3^{a+1}-1)(5^{b+1}-1) = 16 \times 3^a\,5^b.$$

However, the left-hand side of this equation is clearly less than $3^{a+1}5^{b+1} = 15 \times 3^a\,5^b$, so this is a contradiction.

A very similar argument rules out perfect numbers of the form $p_1^{k_1}p_2^{k_2}$ for any odd primes p_1, p_2, showing that an odd perfect number must have at least three prime divisors. In fact, it is known that an odd perfect number, if one exists at all, must have at least eight prime divisors.

4. For this question, let $f(n)$ be the *product* of the positive integer divisors of n.

(a) Find $f(2)$, $f(3)$, $f(6)$. Is f a multiplicative function?

Solution: We have

$$f(2) = 1 \times 2 = 2, \quad f(3) = 1 \times 3 = 3, \quad f(6) = 1 \times 2 \times 3 \times 6 = 36.$$

Since 2 and 3 are coprime to each other but $f(2\times 3) \neq f(2)f(3)$, we conclude that f is not a multiplicative function.

*(b) Express $f(n)$ in terms of n and $\tau(n)$. (Hint: the first question of Tutorial 1 is relevant here.)

Solution: As seen in Q1 of Tutorial 1, if d is a divisor of n then n/d is also a divisor of n. So if n is not a square, the divisors of n occur in pairs $\{d, n/d\}$, which is why the total number of divisors $\tau(n)$ is even for non-square n. (Incidentally, note that this can also be seen from the formula for

$\tau(n)$ in terms of the prime factorization of n: if n is not a square then one of the exponents k_i must be odd, so $\tau(n)$ is a multiple of the even number $k_i + 1$.) We have $\tau(n)/2$ pairs of divisors, and the product of each pair is n, so $f(n) = n^{\tau(n)/2}$ if n is not a square.

If n is a square, then we have $(\tau(n) - 1)/2$ pairs of divisors as above, and one unpaired divisor $\sqrt{n}$. So

$$f(n) = n^{(\tau(n)-1)/2}\sqrt{n} = n^{\tau(n)/2}.$$

Thus the formula $f(n) = n^{\tau(n)/2}$ holds for all positive integers n.

5. Primes p satisfy $\phi(p) = p - 1$. Which positive integers n satisfy $\phi(n) = n - 2$?

Solution: Obviously we only need to consider composite numbers n. The smallest composite number is 4, which indeed has $\phi(4) = 2 = 4 - 2$. After you work out $\phi(6) = 2$, $\phi(8) = 4$, $\phi(9) = 6$, $\phi(10) = 4$, you probably begin to suspect that there are no other solutions of $\phi(n) = n - 2$.

To prove this, suppose that n was a composite number satisfying $\phi(n) = n - 2$. By definition of $\phi(n)$, this means that all but two of the numbers $0, 1, 2, \ldots, n - 1$ are coprime to n. Since $n > 1$, it is certainly not true that 0 is coprime to n (rather, $\gcd(0, n) = n$). So there is exactly one element of $\{1, 2, \cdots, n - 1\}$ which is not coprime to n. Since n is composite, we can write $n = de$ where $d, e \in \{2, 3, \cdots, n - 1\}$. But then neither d nor e is coprime to n, because $\gcd(d, n) = d$ and $\gcd(e, n) = e$. This seems like a contradiction, but isn't quite: the only way out is that d must equal e, so $n = d^2$, and d is the one element of $\{1, 2, \cdots, n - 1\}$ that is not coprime to n. But $2d$ is not coprime to n either (since d divides both of them), so $2d$ must be bigger than $n - 1$, which means that $2d \geq n = d^2$, forcing $d = 2$ and hence $n = 4$.

***6.** Suppose that p is a prime number such that $p \equiv 3 \pmod 4$. Show that there is no integer x such that $x^2 \equiv -1 \pmod p$. (Hint: use Fermat's Little Theorem.)

Solution: Suppose for a contradiction that $x \in \mathbb{Z}$ satisfied $x^2 \equiv -1 \pmod p$. Since $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is an odd integer. So if we raise both sides of the congruence $x^2 \equiv -1 \pmod p$ to the $(\frac{p-1}{2})$th power, we get $x^{p-1} \equiv -1 \pmod p$. However, Fermat's Little Theorem tells us that $x^{p-1} \equiv 1 \pmod p$, since clearly x is not a multiple of p given that $x^2 \equiv -1 \pmod p$. So $1 \equiv -1 \pmod p$, which is a contradiction (since certainly $p \neq 2$).

Extra Exercises:

7. What is the smallest positive integer n such that $\tau(n) = 8$?

Solution: Arguing as in Q2, we see that a positive integer n has $\tau(n) = 8$ if and only if n has one of the following types of prime factorization: $n = p_1^7$, $n = p_1^3 p_2$, or $n = p_1 p_2 p_3$. The smallest numbers of these forms are, respectively, $2^7 = 128$, $2^3\,3 = 24$, and $2 \times 3 \times 5 = 30$. So the answer is 24.

*8. Suppose that p is a prime number such that $p \equiv 1 \pmod 4$.

(a) By considering the product

$$2 \times 4 \times 6 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+3}{2}\right) \times \cdots \times (p-5) \times (p-3) \times (p-1)$$

of all the even integers from 2 to $p-1$ inclusive, show that

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod p.$$

Solution: The product of all the even integers from 2 to $p-1$ inclusive has $\frac{p-1}{2}$ terms. Taking a factor of 2 out of each of these terms, we would get the product of all the integers from 1 to $\frac{p-1}{2}$, which is written $(\frac{p-1}{2})!$. So the product in the question equals $2^{\frac{p-1}{2}}(\frac{p-1}{2})!$.

On the other hand, modulo p, the $\frac{p-1}{4}$ factors in the second half of the product are congruent to the negative numbers $-\frac{p-3}{2}, \cdots, -5, -3, -1$, i.e. all the negative odd integers from $-\frac{p-3}{2}$ to -1 inclusive. Apart from the minus signs, these are exactly the odd integers which together with $2, 4, \cdots, \frac{p-1}{2}$ make up the factors in $(\frac{p-1}{2})!$. Hence

$$2^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{4}} \left(\tfrac{p-1}{2}\right)! \pmod p.$$

Since p is prime, all the factors in $(\frac{p-1}{2})!$ are coprime to p, so we can invoke coprime cancellation to cancel $(\frac{p-1}{2})!$ from both sides of this congruence to deduce the desired result.

(b) Note that we either have $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$. Show that if $p \equiv 5 \pmod 8$, there is no integer x such that $x^2 \equiv 2 \pmod p$.

Solution: Suppose for a contradiction that $p \equiv 5 \pmod 8$ and $x^2 \equiv 2 \pmod p$ for some integer x. The assumption that $p \equiv 5 \pmod 8$ means that $\frac{p-1}{4}$ is odd, so the previous part tells us that $2^{\frac{p-1}{2}} \equiv -1 \pmod p$. We deduce that $x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv -1 \pmod p$. However, Fermat's Little Theorem tells us that $x^{p-1} \equiv 1 \pmod p$, since clearly x is not a multiple of p given that $x^2 \equiv 2 \pmod p$. So $1 \equiv -1 \pmod p$, which is a contradiction (since certainly $p \neq 2$).

**9. Let n be a positive integer. Show that $\sigma(n) + \phi(n) \geq 2n$, with equality if and only if n is either prime or equal to 1. (Hint: write $n = p^k m$ where p is a prime factor of n and $\gcd(p, m) = 1$, and find a lower bound for $\sigma(n) + \phi(n)$ in terms of $\sigma(m) + \phi(m)$.)

Solution: We prove this by (strong) induction on n. When $n = 1$, the claim is true: $\sigma(1) + \phi(1) = 1 + 1 = 2$, so this claimed case of equality does hold.

We can assume from now on that $n > 1$ and that the claim is known when n is replaced by any smaller positive integer. Following the hint, we focus on one prime factor p of n, and let p^k be the highest power of p that divides n (thus, $k \geq 1$),

so that $n = p^k m$ where $\gcd(p, m) = 1$. Since σ and ϕ are both multiplicative functions,

$$\begin{aligned}
\sigma(n) + \phi(n) &= \sigma(p^k m) + \phi(p^k m) \\
&= \sigma(p^k)\sigma(m) + \phi(p^k)\phi(m) \\
&= (1 + p + p^2 + \cdots + p^k)\sigma(m) + (p^k - p^{k-1})\phi(m) \\
&\geq (p^k + p^{k-1})\sigma(m) + (p^k - p^{k-1})\phi(m) \\
&= p^k(\sigma(m) + \phi(m)) + p^{k-1}(\sigma(m) - \phi(m)) \\
&\geq p^k(\sigma(m) + \phi(m)).
\end{aligned}$$

The justification for the first inequality in this calculation is easy: we replaced the whole geometric series $1 + p + p^2 + \cdots + p^k$, which has $k + 1 \geq 2$ terms, with the sum of its two biggest terms, and this was all multiplied by $\sigma(m)$ which is positive. In particular, equality holds in this step if and only if $k = 1$. The justification for the second inequality is that $\sigma(m) \geq \phi(m)$, because $\sigma(m) \geq m$ (as m is one of the divisors of which $\sigma(m)$ is the sum) and $m \geq \phi(m)$ (by definition of $\phi(m)$). In particular, equality holds in this step if and only if $m = 1$. We have thus proved that

$$\sigma(n) + \phi(n) \geq p^k(\sigma(m) + \phi(m)),$$

with equality if and only if $k = 1$ and $m = 1$, i.e. if and only if $n = p$ is prime.

Since $m < n$, the induction hypothesis applies to m. So $\sigma(m) + \phi(m) \geq 2m$, with equality holding if and only if m is either prime or equal to 1. Hence

$$\sigma(n) + \phi(n) \geq p^k(\sigma(m) + \phi(m)) \geq 2p^k m = 2n,$$

with equality holding throughout if and only if $n = p$ is prime (and thus $m = 1$). This completes the proof.