Problem 1, TFJM

Equipe d'Orsay

June 29, 2012

In this paper we study some multiplicative functions and the Dirichlet's convloution product which leads us to establish some beautiful formulae implying the Euler's totient function and the number of divisors function.

We solved the first four questions of the problem and studied the fifth for n - a prime number using some theory about cyclotomic polynomials. Also we considered the question six in the case where $m = p + 1$ with p - a prime number.

0.1 Multiplicative functions

For two arithmetic functions $f, g : \mathbf{N}^* \to \mathbf{C}$, define their convolution product $f * g$ by

$$f * g(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Say that f is multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. Then, if f and g are multiplicative, so is $f * g$. Indeed, the fact that $\gcd(m, n) = 1$ implies that any divisor of mn can be uniquely written as a product of a divisor of m and a divisor of n, hence

$$f * g(mn) = \sum_{d_1|m, d_2|n} f(d_1 d_2) g\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right) = \sum_{d_1|m, d_2|n} f(d_1) g\left(\frac{m}{d_1}\right) f(d_2) g\left(\frac{n}{d_2}\right)$$

$$= \left(\sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right)\right) \cdot \left(\sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right)\right) = (f * g)(m) \cdot (f * g)(n).$$

By taking $g = 1$, we obtain that $f * 1$ is multiplicative whenever f is. Note that $f * 1(n) = \sum_{d|n} f(d)$, that is the kind of sum we are concerned with in this problem. Note that if $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$ is the prime factorization of n (where p_i are distinct prime numbers and α_i are positive integers), then for any multiplicative map f we have

$$f(n) = \prod_{i=1}^{m} f(p_i^{\alpha_i}).$$

By taking $f = \tau$, we have $f(p^k) = k + 1$ for all primes p and all $k \geq 0$, hence

$$\tau(n) = \prod_{i=1}^{m} (1 + \alpha_i) \quad \text{if} \quad n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}.$$

By taking $f = \varphi$, the Euler's totient function, we obtain

$$\sum_{d|p^k} \varphi(d) = 1 + (p-1) + p(p-1) + ... + p^{k-1}(p-1) = p^k,$$

hence by the previous discussion

$$\sum_{d|n} \varphi(d) = n.$$

Finally, by taking $f = \tau$, we obtain

$$\sum_{d|p^k} f(d) = \sum_{j=0}^{k} (j+1) = \frac{(k+1)(k+2)}{2},$$

hence

$$\sum_{d|n} \tau(d) = \prod_{i=1}^{m} \frac{(\alpha_i + 1)(\alpha_i + 2)}{2} \quad \text{if} \quad n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}.$$

0.2 Question 1 a)

Let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$$

be the prime factorization of n. Taking into account the results of the previous section, namely the formulae

$$\tau(n) = \prod_{i=1}^{m} (1+\alpha_i), \quad \sum_{d|n} \tau(d) = \prod_{i=1}^{m} \frac{(\alpha_i+1)(\alpha_i+2)}{2},$$

we obtain that n is τ-perfect if and only if

$$2\tau(n) = \sum_{\substack{d|n \\ 1\le d\le n}} \tau(d) = \tau(n) \prod_{i=1}^{m} \frac{(\alpha_i+2)}{2} \Leftrightarrow \prod_{i=1}^{m} (\alpha_i+2) = 2^{m+1}$$

As by assumption all α_i are positive, the previous relation is equivalent to $m = 1$ and $\alpha_1 = 2$, that is n is the square of a prime. Hence the τ-perfect numbers are precisely the squares of prime numbers.

0.3 Question 1. b)

Consider first the case $k \geq 1$. We will prove that there are no solutions to the following equation :

$$\tau(n) + k = \sum_{\substack{d|n \\ 1\le d\le n-1}} (\tau(d) + k).$$

Firstly, the equation can be rewritten as :

$$\tau(n)(1-k) + 2k = 1 + \sum_{\substack{d|n \\ 2\le d\le n-1}} \tau(d)$$

and because

$$\sum_{\substack{d|n \\ 2\le d\le n-1}} \tau(d) \geq 2(\tau(n) - 2)$$

we conclude that

$$\tau(n) \leq \frac{2k+3}{k+1} = 2 + \frac{1}{k+1} \leq 3.$$

Also it is not difficult to see that no n for which $\tau(n) \in \{1, 2, 3\}$ is $(\tau + k)$-perfect, which proves the desired result.

Consider now the equation

$$2\tau(n) - 2k = \sum_{\substack{d|n \\ 1\le d\le n}} (\tau(d) - k),$$

where k is positive.

Let, as before $n = \prod_{i=1}^{m} p_i^{\alpha_i}$ be the prime factorization of n. The above equation is equivalent to

$$\tau(n)(2+k) - 2k = \sum_{\substack{d|n \\ 1\le d\le n}} \tau(d) = \prod_{i=1}^{m} \frac{(\alpha_i+1)(\alpha_i+2)}{2}$$

and also to

$$\tau(n)(2^m k + 2^{m+1} - \prod_{i=1}^{m}(\alpha_i+2)) = 2^{m+1}k.$$

Let's now consider the case where k is a power of 2. We can write then : $k = 2^r$, where r is a positive integer($r \geq 1$). Saying that it exists a $(\tau(n) - 2^r)$-perfect n is equivalent to solving the following equation.

We assume that this equality holds for some $m, \alpha_i, r > 0$,.

$$\tau(n)(2^{m+r} + 2^{m+1} - \prod_{i=1}^{m}(\alpha_i+2)) = 2^{m+r+1}.$$

Then we have : $\gcd(2^{m+r} + 2^{m+1} - \prod_{i=1}^{m}(\alpha_i+2)\ ,\ 2^{m+r+1})$=1 because $\tau(n)$ is power of 2 and then all the α_i are odd , so we deduce that $\prod_{i=1}^{m}(\alpha_i+2)$ is also odd.

So then as $\tau(n)|2^{m+r+1}$ and by the Gauss theorem $2^{m+r+1}|\tau(n)$, we deduce that $\tau(n) = 2^{m+r+1}$ and

$$2^{m+r} + 2^{m+1} - \prod_{i=1}^{m}(\alpha_i+2) = 1.$$

Now like $\prod_{i=1}^{m}(\alpha_i+2) > \tau(n)$ we obtain :

$$2^{m+r} + 2^{m+1} - 1 > 2^{m+r+1}$$

say $2^m(2-2^r) > 1$ which is clearly impossible because $r \geq 1$ and then $(2-2^r) \leq 0$ So we conclude that if k is a power of 2 our equation do not have integer solutions and it do not exists a $(\tau(n) - 2^r)$-perfect n.

We can also consider the case $k = 1$, when the previous equation becomes:

$$\tau(n)(3.2^m - \prod_{i=1}^{m}(\alpha_i+2)) = 2^{m+1}$$

As

$$\tau(n) = \prod_{i=1}^{m}(\alpha_i+1) \geq 2^m,$$

and $\tau(n)$ divides 2^{m+1}, we obtain $\tau(n) = 2^m$ or $\tau(n) = 2^{m+1}$. In the first case we must have $\alpha_i = 1$ for all i and the equation becomes $3 \cdot 2^m - 3^m = 2$, with no positive solutions (work modulo 3). In the second case we have $\tau(n) = 2^{m+1}$. But then

$$(\alpha_i+1)2^{m-1} \leq \prod_{i=1}^{m}(\alpha_i+1) = 2^{m+1}.$$

We deduce that all α_i are equal to $1, 2$ or 3. Clearly none of them is equal to 2, and we deduce that $m-1$ of the α_i's are equal to 1 and one of them is equal to 3. Hence the equation becomes

$$3 \cdot 2^m - 5 \cdot 3^{m-1} = 1$$

and it has only one solution, namely $m = 1$ (as if $m > 1$, the left hand-side is a multiple of 3). We deduce that $m = 1$ and $\alpha_1 = 3$, that is $n = p^3$ for some prime p. Conversely, it is clear that any such number is a solution of the problem.

0.4 Question 2

We saw in the first section that

$$\sum_{d|n} \varphi(d) = n.$$

So n is φ-perfect if and only if $2\varphi(n) = n$. Write $n = 2^k q$ with $k \geq 1$ and q an odd integer. Then $\varphi(n) = \varphi(q)\varphi(2^k) = 2^{k-1}\varphi(q)$, so the equation becomes $\varphi(q) = q$. This clearly happens if and only if $q = 1$, that is $n = 2^k$. So n is φ-perfect if and only if n is a power of 2.

0.5 Question 3

Assume that $n = 2^k(2^{k+1} - 2k - 1)$ and that $2^{k+1} - 2k - 1$ is a prime. Then :

$$\sum_{\substack{d|n \\ 1 \leq d \leq n-1}} (d-1) = -(\tau(n) - 1) + \sum_{\substack{d|n \\ 1 \leq d \leq n-1}} d$$

$$= (\sum_{i=0}^{k} 2^i) + (2^{k+1} - 2k - 1)(\sum_{i=0}^{k-1} 2^i) - (\tau(n) - 1).$$

But

$$\tau(n) = \tau(2^k)\tau(2^{k+1} - 2k - 1) = 2(k+1)$$

so finally we have :

$$\sum_{\substack{d|n \\ 1 \leq d \leq n-1}} (d-1) = 2^{k+1} - 1 + (2^{k+1} - 2k - 1)(2^k - 1) - 2k - 1 = n - 1$$

and therefore n is $(n-1)$-perfect.

Let's study the general case , where $f(n) = n + a$, with $a \in \mathbb{Z}$. We want to find solutions of the form $n = 2^k p$, where p is a prime number. Then $\tau(n) = 2(k+1)$ and we have :

$$\sum_{\substack{d|n \\ 1 \leq d \leq n-1}} (d+a) = (\sum_{i=0}^{k} 2^i) + p(\sum_{i=0}^{k-1} 2^i) + (\tau(n) - 1)a$$

So, we obtain :

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

from where we conclude that we must have :

$$p = 2^{k+1} + 2ak - 1$$

Conversely, if $(2^{k+1} + 2ak - 1)$ is prime then $n = 2^k(2^{k+1} + 2ak - 1)$ is $n + a$ - perfect.

0.6 Question 4

We have $f(n) = ln(n)$, hence n is f-perfect if and only if

$$2ln(n) = \sum_{d|n} ln(d) \Longleftrightarrow ln(n^2) = ln(\prod_{d|n} d)$$

$$\Longleftrightarrow n^2 = \prod_{d|n} d$$

Let $n \geq 2 \mid n = \prod_{i=1}^{r} p_i^{\alpha_i}$, we will compute $P(n) = \prod_{d|n} d$

A positive divisor of n, can be written as $d = \prod_{i=1}^{r} p_i^{\beta_i}$ with $0 \leq \beta_i \leq \alpha_i$. The product $P(n)$ is then:

$$P(n) = \prod_{i=1}^{r} p_i^{\gamma_i}$$

Let be $v \in \{0, 1, \cdots, \alpha_1\}$. There is $\dfrac{\tau(n)}{\alpha_1 + 1}$ divisors of n for which $\beta_1 = v$.When we multiply all this divisors , one obtain:

$$\gamma_1 = \frac{\tau(n)}{\alpha_1 + 1} \sum_{v=0}^{\alpha_1} v = \alpha_1 \frac{\tau(n)}{2}$$

The same is happening for all γ_i. We get

$$P(n) = n^{\frac{\tau(n)}{2}}$$

So for $n \geq 2$, n is f-perfect $\Longleftrightarrow n^2 = n^{\frac{\tau(n)}{2}}$, i.e $\tau(n) = 4$

We have $n = p^3$ or $n = pq$, where p and q are two distinct prime numbers.
Considering the case $n = 1$, gives us $2ln(1) = 0 = \sum_{d|1} ln(d)$, So 1 is f-perfect.

Finally are f-perfect for $f(n) = ln(n)$ the integers:

$$\{1, p^3, pq \mid p, q \in P, p \neq q\}$$

where P is the set of prime numbers.

0.7 Question 5

If n is f-perfect for $f(n) = (-1)^n$, then n is even, because the case where n is odd is obvious and leads us to the set of all odd prime numbers as answer, so we can write $n = 2^k q$ for an odd integer q. The odd divisors of n are the divisors of q, hence n has $\tau(q)$ odd divisors. Since $\tau(n) = (k+1)\tau(q)$, it follows that n has $k\tau(q)$ even divisors. We deduce that n is f-perfect if and only if

$$2 = \sum_{d|n} (-1)^d = k\tau(q) - \tau(q) \Leftrightarrow \tau(q) = \frac{2}{k-1}.$$

In particular, we must have $k \in \{2, 3\}$. If $k = 2$, then q must be a prime and so $n = 4p$, where p is an odd prime number. If $k = 3$, then $q = 1$ and so $n = 8$.

Hence n is f-perfect for $f(n) = (-1)^n$ if and only if $n = 8$, or $n = 4p$, or $n = p$ with p an odd prime number.

0.7.1 Preliminaries on roots of unity

We will need some theory about cyclotomic polynomials to solve the case where w is a root of unity. We solved the case where w is a p -th root of unity where p is prime.

Let Φ_n be the nth cyclotomic polynomial.

Théorème 0.1. *The polynomial Φ_n has integer coefficients and is irreducible in $\mathbf{Q}[X]$.*

The fact that Φ_n has integer coefficients follows by induction from the identity

$$\prod_{d|n} \Phi_d = X^n - 1,$$

which is a consequence of the fact that any nth root of unity is a primitive root of order d for a unique $d|n$. The irreducibility assertion is much harder and we will admit it. When n is a prime, the proof is easier, since we can apply directly Eisenstein's irreducibility criterion to $\Phi_p(X+1)$.

Corollaire 0.2. *If $f \in \mathbf{Q}[X]$ is a polynomial such that $f(\zeta_n) = 0$, then Φ_n divides f.*

Proof. Since Φ_n is irreducible in $\mathbf{Q}[X]$, we have $\gcd(f, \Phi_n) \in \{1, \Phi_n\}$. We cannot have $\gcd(f, \Phi_n) = 1$, as otherwise there would be $A, B \in \mathbf{Q}[X]$ such that $Af + B\Phi_n = 1$ and evaluating at ζ_n would yield $0 = 1$. Hence $\gcd(f, \Phi_n) = \Phi_n$ and Φ_n divides f. □

We will frequently use the following result, which is just a translation of the previous corollary:

Lemme 0.3. *Let p be a prime and let $a_0, a_1, ..., a_{p-1} \in \mathbf{Q}$. Then $a_0 + a_1\zeta_p + ... + a_{p-1}\zeta_p^{p-1} = 0$ if and only if $a_0 = a_1 = ... = a_{p-1}$.*

Proof. One implication is immediate, since

$$1 + \zeta_p + ... + \zeta_p^{p-1} = \frac{\zeta_p^p - 1}{\zeta_p - 1} = 0.$$

For the other implication, the corollary shows that $a_0+a_1X+...+a_{p-1}X^{p-1}$ is a multiple of $\Phi_p = \frac{X^p-1}{X-1} = X^{p-1}+X^{p-2}+...+X+1$. Since it has degree at most $p-1$, there must exist a constant c such that $a_0+a_1X+...+a_{p-1}X^{p-1} = c\Phi_p$, and the result follows. $\square$

Let's consider the case where $\omega = e^{\frac{2i\pi}{p}}$ with p-a prime number. Assume first that $p = 3$ and let's treat this case. From the definition of a f-perfect number for $f(n) = \omega^n$ we have :

$$2\omega^n = \sum_{d|n} \omega^d$$

Let's now define the following sets :

$$D_1 = \{d_1 > 0, d_1|n, d_1 \equiv 1 mod 3\}$$

$$D_2 = \{d_2 > 0, d_2|n, d_2 \equiv 2 mod 3\}$$

And their cardinals : $n_1 = \#D_1$ and $n_2 = \#D_2$. Note that $n_1 \geq 1$ because $1 \in D_1$

It is clear that if $n \neq 3k$, with k a positive integer then :

$$2\omega^n = n_1\omega + n_2\omega^2$$

In particular if $n \equiv 1$ mod 3 then we have : $2\omega = n_1\omega + n_2\omega^2$ hence $2 = n_1 + n_2\omega$, so $n_1 = 2$ and $n_2 = 0$ so it's clear , as $1 \in D_1$ that n is a prime such as $n \equiv$1 mod 3.

Assume now that $n \equiv 2$ mod 3. Then from our first equality it follows :

$2\omega^2 = n_1\omega + n_2\omega^2$ say $2\omega = n_1 + n_2\omega$ which leads to : $n_1 = 0$ and $n_2 = 2$ which is impossible ($n_1 \geq 1$).

Finally if $n = 3^\alpha m$, with gcd$(m, 3)$=1 and $\alpha \geq 1$,

$$2 = n_1\omega + n_2\omega^2 + \alpha\tau(m)$$

Let's now define the polynomial $P(X) = n_2X^2 + n_1X + (\alpha\tau(m) - 2)$ then ω is a root of $P(X)$, so by the previous lemma we have :

$$n_1 = n_2 = \alpha\tau(m) - 2$$

since $\Phi_3 = X^2 + X + 1$. Clearly we have $\tau(m) = n_1 + n_2$ and therefore

$$N := n_1 = n_2 = 2\alpha N - 2$$

So $N(2\alpha - 1) = 2$. But $\alpha \geq 1$ and the only solution is $N = n_1 = n_2 = 2$ and $\alpha = 1$. We conclude that $n = 3pq$ where p and q are prime numbers such that $p \equiv 1$ mod 3 and

$q \equiv 2 \bmod 3$. Conversely these are solutions (cf our calculus which are necessary and sufficient conditions).

Conclusion : The solutions are $n = p$ where p is a prime $\equiv 1 \bmod 3$ and $n = 3pq$ where p and q are primes such that $p \equiv 1 \bmod 3$ and $q \equiv 2 \bmod 3$.

Assume now that p is a prime with $p \geq 5$, then we define like previously for $0 \leq k \leq p-1$:

$$D_k = \{d > 0, d|n, d \equiv kmodp\}$$

$$n_k = Card(D_k)$$

With these notations, we have :

$$2\omega^n = n_0 + n_1\omega + n_2\omega^2 + ... + n_{p-1}\omega^{p-1}$$

Assume now that $n \equiv r \bmod p$ with $1 \leq r \leq p-1$. Then

$$n_{p-1}\omega^{p-1} + ... + (n_r - 2)\omega^r + ... + n_1\omega = 0$$

Because this is a polynomial equation of degree $p-1$ on w, we must have :

$$n_{p-1} = ... = (n_k - 2) = ... = n_1 = 0$$

(Note that the constant coefficient of the polynomial is 0).

To conclude, $n_i = 0$ if $i \neq r$ and $n_r = 2$. But $n_1 \geq 1$ (because $1 \in D_1$) and so $r = 1$. Therefore n is prime and $n \equiv 1 \bmod p$, and conversely it is a solution, like before.

Finally, we assume that $n = p^\alpha m$ with $\alpha \geq 1$ and $gcd(m,p) = 1$. Then we have

$$(n_0 - 2) + n_1\omega + n_2\omega^2 + ... + n_{p-1}\omega^{p-1} = 0$$

with $n_0 = \alpha(n_1 + ... + n_{p-1})$, like in the case $p = 3$. Therefore $N := n_1 = n_2 = ... = n_{p-1} = n_0 - 2$. But $n_0 = (p-1)\alpha N$. So $N = (p-1)\alpha N - 2$, i.e $N((p-1)\alpha - 1) = 2$. But $(p-1)\alpha - 1 \geq 4 - 1 = 3$, impossible.

To conclude, the only solutions in the case $p > 3$ are n prime with $n \equiv 1 \bmod p$.

0.8 Question 6

Let's cosider $m = p + 1$ where p is a prime number. Then our equality can be written as :

$$2\binom{m}{n} = \sum_{d|n} \binom{m}{d}$$

It's easy to see that it doesn't hold for $n = 1$ or $n = m$. Let's prove that it holds if and only if $n = p$. Since one implication is obvious , let's suppose that our equality holds for $2 \leq n \leq p-1$. Now , it's clear that $\binom{p+1}{n}$ is equal to 0 modulo p for all $2 \leq n \leq p-1$, but $\sum_{d|n} \binom{m}{d} = 1 \mod p$, so we obtain a contradiction and we conclude that the only solution for $m = p + 1$ with p - a prime number is $n = p$. We can now consider the case where $m = 2011 + 1 = 2012$. Since 2011 is prime , we conclude that the only solution to the equality :

$$2\binom{2012}{n} = \sum_{d|n} \binom{2012}{d}$$

is $n = 2011$.