

Evaluating ϕ , τ and σ

MATH2068 Number Theory & Cryptography
Week 5 Lecture 2

University of Sydney
NSW 2006
Australia

26th August 2008

Expressing integers as coprime products



By the Fundamental Theorem of Arithmetic, every positive integer is uniquely expressible as a product of primes.

So if $n \in \mathbb{Z}^+$ there exist pairwise distinct primes p_1, p_2, \dots, p_r and positive integer exponents k_1, k_2, \dots, k_r such that

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

(If $n = 1$ then $r = 0$, giving an “empty product”.)

Let $m_i = p_i^{k_i}$, so that $n = m_1 m_2 \cdots m_r$.

Since the p_i are pairwise distinct,
 $\gcd(m_1, m_2 m_3 m_4 \cdots m_r) = 1$, $\gcd(m_2, m_3 m_4 \cdots m_r) = 1$,
 $\gcd(m_3, m_4 \cdots m_r) = 1$, etc.

Evaluating multiplicative functions



Recall the definition:

A function f defined on the positive integers is said to be *multiplicative* if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

If $n = m_1 m_2 \cdots m_r$ as above, then

$$\begin{aligned} f(n) &= f(m_1) f(m_2 m_3 \cdots m_r) \\ &= f(m_1) f(m_2) f(m_3 \cdots m_r) \\ &\vdots \\ &= f(m_1) f(m_2) f(m_3) \cdots f(m_r). \end{aligned}$$

So we can evaluate $f(n)$ for any $n \in \mathbb{Z}^+$ if we can evaluate $f(m)$ when m is a prime power.

Euler phi



Let's evaluate $\phi(12000)$ (the number of numbers less than 12000 and coprime to 12000).

$$12000 = 12 \times 10^3 = 2^2 \times 3 \times (2 \times 5)^3 = 2^5 \times 3 \times 5^3.$$

So $\phi(12000) = \phi(2^5) \phi(3) \phi(5^3)$.

In fact $\phi(2^5) = 16$, $\phi(3) = 2$ and $\phi(5^3) = 100$
 So the answer is $\phi(12000) = 3200$.

But what is $\phi(p^k)$, in general, when p is prime?

Euler phi of a prime power



If p is a prime and $k \in \mathbb{Z}^+$ then $\gcd(r, p^k) > 1$ if and only if $p|r$.

The r in $\{0, 1, 2, \dots, p^k - 1\}$ with $\gcd(r, p^k) > 1$ are exactly $0, p, 2p, 3p, \dots, p^k - p$.

These are the numbers ip for i from 0 to $p^{k-1} - 1$ inclusive. There are exactly p^{k-1} of them.

All the other natural numbers less than p^k are coprime to p^k .

So $\phi(p^k) = p^k - p^{k-1}$.

Alternatively expressed, $\phi(p^k) = p^k(1 - \frac{1}{p})$.

$(1/p)$ -th of the numbers less than p^k are not coprime to p^k , $((p-1)/p)$ -ths of them are coprime to p^k .

General formula for $\phi(n)$.



If you can factorize n then it is easy to compute $\phi(n)$:

If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where the p_i are distinct primes, then

$$\begin{aligned}\phi(n) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \dots \phi(p_r^{k_r}) \\ &= p_1^{k_1} \left(1 - \frac{1}{p_1}\right) p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \dots p_r^{k_r} \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

We can also write this as

$$\phi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

(The pi notation (\prod) is like sigma notation (\sum), but for products instead of sums. e.g. $\prod_{i=1}^n s_i \stackrel{\text{def}}{=} s_1 s_2 \dots s_n$.)

Is this computationally efficient?



In a word, “**no**”.

There is no known computationally efficient way to calculate $\phi(n)$ without factorizing n .

And factorization is computationally difficult for large numbers with few prime factors.

The security of the RSA cryptosystem depends on the fact that if a number n is the product of two very large primes p and q , then it is practically impossible to find p and q given only n , and, in consequence, it is practically impossible to calculate $\phi(n)$.

The number of divisors function



If p is prime the divisors of p^k are $1, p, p^2, \dots, p^k$.

So $\tau(p^k) = k + 1$.

So if $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ then

$$\begin{aligned}\tau(n) &= \tau(p_1^{k_1})\tau(p_2^{k_2}) \dots \tau(p_r^{k_r}) \\ &= (k_1 + 1)(k_2 + 1) \dots (k_r + 1).\end{aligned}$$

For example,

$$\tau(12000) = \tau(2^5 \times 3^1 \times 5^3) = 6 \times 2 \times 4 = 48.$$

(You can easily write down all the divisors of 12000 if you want: $2^0 \times 3^0 \times 5^0, 2^1 \times 3^0 \times 5^0, \dots, 2^5 \times 3^1 \times 5^3$.)

The sum of divisors function



If p is prime the divisors of p^k are $1, p, p^2, \dots, p^k$.

$$\text{So } \sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

So if $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ then

$$\begin{aligned} \sigma(n) &= \sigma(p_1^{k_1}) \sigma(p_2^{k_2}) \dots \sigma(p_r^{k_r}) \\ &= \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right). \end{aligned}$$

For example,

$$\begin{aligned} \sigma(12000) &= \sigma(2^5 \times 3^1 \times 5^3) \\ &= \left(\frac{2^6 - 1}{1} \right) \left(\frac{3^2 - 1}{2} \right) \left(\frac{5^4 - 1}{4} \right) \\ &= 63 \times 8 \times 156 \\ &= 78624. \end{aligned}$$

Perfect numbers



Definition: A number is called *perfect* if it is the sum of its proper divisors.

For example, the divisors of 6, excluding 6, are 1, 2, 3.

$$\text{And } 1 + 2 + 3 = 6.$$

The proper divisors of 28 are 1, 2, 4, 7, 14.

$$\text{And } 1 + 2 + 4 + 7 + 14 = 28.$$

The next one is 496, with proper divisors 1, 2, 4, 8, 16, 31, 62, 124 and 248.

It is not known if there are any perfect numbers that are *odd*.

But it is known that any odd perfect number would have to exceed 10^{300} ; so you won't find one easily!

Classifying even perfect numbers



Recall that n is perfect if n is the sum of the divisors of n , excluding n .

The sum of *all* the divisors of n will equal $2n$.

i.e. n is perfect if $\sigma(n) = 2n$.

Suppose that n is even and perfect. Then we can write $n = 2^k m$, where $k \geq 1$ and m is odd. (Here m is the product of the odd prime divisors of n .)

Since n is perfect,

$$2^{k+1} m = 2n = \sigma(n) = \sigma(2^k m) = \sigma(2^k) \sigma(m)$$

(the last step because $\gcd(2^k, m) = 1$ and σ is multiplicative).

Classifying even perfect numbers (continued)



Let n be perfect, $n = 2^k m$ with m odd and $k \geq 1$. Then

$$\begin{aligned} 2^{k+1} m = 2n &= \sigma(n) = \sigma(2^k m) \\ &= \sigma(2^k) \sigma(m) = (2^{k+1} - 1) \sigma(m) \end{aligned} \quad (*)$$

and so $(2^{k+1} - 1) | 2^{k+1} m$.

But $\gcd(2^{k+1} - 1, 2^{k+1}) = 1$. So $(2^{k+1} - 1) | m$.

Write $m = r(2^{k+1} - 1)$. Then (*) gives

$$2^{k+1} r(2^{k+1} - 1) = (2^{k+1} - 1) \sigma(m)$$

and so $\sigma(m) = r 2^{k+1} = r(2^{k+1} - 1) + r = r + m$.

But if $r > 1$ then 1, r and m are distinct divisors of m , and so $\sigma(m) \geq 1 + r + m$ — contradiction.

So $r = 1$, and $n = 2^k m = 2^k (2^{k+1} - 1)$.

Classifying even perfect numbers (concluded)



On the last page we showed that if n is an even perfect number then $n = 2^k(2^{k+1} - 1)$ for some positive integer k .

We can say more than this!

Writing $m = 2^{k+1} - 1$, we have $n = 2^k m$ and

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

So $\sigma(m) = 2^{k+1} = m + 1$.

This means that 1 and m are the *only* divisors of m .

That is, m must be prime.

Conclusion



The conclusion is that if n is an even perfect number then $n = 2^k(2^{k+1} - 1)$, where $2^{k+1} - 1$ must be prime.

Conversely, if $2^{k+1} - 1$ is prime then $2^k(2^{k+1} - 1)$ is indeed perfect.

This is easily checked. Writing $m = 2^{k+1} - 1$ again,

$$\begin{aligned} \sigma(n) = \sigma(2^k m) &= \sigma(2^k)\sigma(m) = (2^{k+1} - 1)(m + 1) \\ &= (2^{k+1} - 1)2^{k+1} = 2^{k+1} m = 2n, \end{aligned}$$

and so n is perfect.

Prime numbers that are one less than a power of 2 are called *Mersenne primes*.

There are exactly 44 Mersenne primes known. See the [Great Internet Mersenne Prime Search](#) home page.