Dr. Marques Sophie
Office 519

Number theory

Fall Semester 2013
marques@cims.nyu.edu

Problem Set #8

Due monday november 4th in Class

Exercise 1: $(\star)$ 4 points
Let ϕ be Euler's function. Show that $\phi(n^m) = n^{m-1}\phi(n)$ for all natural number n, m.
Solution:
Let $n = p_1^{a_1}...p_r^{a_r}$ be the prime decomposition for n. Since ϕ is multiplicative on coprime elements, we have that $\phi(n^m) = \phi(p_1^{ma^1})....\phi(p_r^{ma_r})$. Next, we know that if q is prime and $k \geq 1$ then $\phi(q^k) = q^{k-1}(q-1)$. Written another way reads $\phi(q^k) = q^{k-1}(q-1)$. Using this with what we have already written we get

$$\phi(n^m) = p_1^{ma_1-1}...p_r^{ma_r-1}\phi(p_1)...\phi(p_r) = \frac{{p_1}^{ma_1}...p_r^{ma_r}}{p_1...p_r}\phi(n) = n^{m-1}\phi(n)$$

where we have used the multiplicativity of ϕ on the primes to get the second equality.

Exercise 2: $(\star)$ 4 points
Let N be a product of two distinct primes. Show that if we know $\varphi(N)$, then we can easily factorize N.
Solution:
Let $N = pq$ where $p < q$ are distinct primes. Then,

$$\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1$$

Define $K := N - \varphi(N) + 1 = p + q$. Note that we can compute K from N and $\varphi(N)$ without knowing p and q. We have

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - Kx + N$$

Thus, by solving the roots of this quadratic polynomial, we obtain that

$$p = \frac{K - \sqrt{K^2 - 4N}}{2} \qquad\qquad q = \frac{K + \sqrt{K^2 - 4N}}{2}$$

In this way, we can obtain prime factorization of N quickly.

Exercise 3: $(\star)$ 4 points
Find the last two digits of the decimal expansion of 3^{1123} (For example the last two digits of 1729 are 29).

Solution:

Notice that finding the last two digits of the 3^{1123} *is equal to finding* w *in the equation:* $3^{1123} \equiv x \ mod\ 100$*, notice that* $gcd(3, 100) = 1$ *so, as it follows from Euler's theorem* $3^{\phi(100)} \equiv 1 \ mod\ 100$*, we will find* $\phi(100)$*:* $100 = 2^2 \times 5^2$*, therefore* $\phi(100) = (2-1) \times 2^{2-1} \times (5-1) \times 5^{2-1} = 40$*, notice that* $1112 = 28 \times 40 + 3$*, therefore* $3^{1123} = (3^{40})^{28} \times 3^3 \equiv 1 \times 3^3 \ mod\ 100 = 27 \ mod\ 100$*, then* $x = 27$*, so the last two digits of* 3^{1123} *are* 27*.*

Exercise 4: $(\star)$ 4 points
Show that there is no solution to the equation $\phi(n) = 14$.

Solution:
Assume that $n = p_1^{t_1} p_2^{t_2} ... p_k^{t_k}$ *is the prime factorization of* n*. Using the the formula derived in class, if then* $\phi(n) = 14$ *means that*

$$14 = p_1^{t_1-1}(p_1 - 1)p_2^{t_2-1}(p_2 - 1)...p_k^{t_k-1}(p_k - 1)$$

On account of the $p_i - 1$ *terms in the expression, the only primes* p_i *in* n *must be such that* $p_i - 1$ *divides* 14*. Thus the only primes possible in* n *are* 2 *and* 3*. This means that* $n = 2^a 3^b$ *where* $0 \leq a, b$ *so that*

$$14 = 2^{a-1} \times 1 \times 3^{b-1} \times 2$$

where the $p^{j-1}(p-1)$ *term is present only if the* p *occurs in the prime factorization of* n*.*
Note that if $b > 1$ *then* $3|14$ *a contradiction thus* $b = 0, 1$*. But if* $b = 1$ *then the equation becomes* $14 = 2^{a-1}3^{1-1}2$ *which implies that* $2^{a-1} = 7$ *which is impossible. Thus* $b = 0$*. But if* $b = 0$ *then then the equation becomes* $14 = 2^{a-1}$ *which once again is impossible. Thus there can be no solution to the equation* $\phi(n) = 12$*.*

Exercise 5: $(\star)$ 4 points
You receive a message that was encrypted using the RSA system with public key $(65, 29)$, where 65 is the base and 29 is the exponent. The encrypted message in two blocks, is 3/2. Find the private key and decrypt the message.

Solution:
First we find $\phi(65)$*. The prime factorization of* 65 *is* 5×13*, hence* $\phi(65) = \phi(5)\phi(13) = (5-1)(13-1) = 48$*. To find* β*, we can apply the Euclidean algorithm to* 29 *and* 48 *and we find* $5 \times 29 - 3 \times 48 = 1$ *which implies that* 5 *is the inverse of* 29 *modulo* 48*. Now that we know the private key, the decrypted message is* b_1/b_2*, where* $b_1 \equiv 3^5 \ mod\ 65$*,* $b_2 \equiv 2^5 \ mod\ 65$*, and* $0 \leq b_1, b_2 < 65$*. We find that* $b_1 = 48$*,* $b_2 = 32$*.*

[1]

[1] $(\star)$ = easy , $(\star\star)$= medium, $(\star\star\star)$= challenge