Hugo *Rincon Galeana*

TU Wien, Winter 2019
104.272 Discrete Mathematics, Group 1 (Professor Gittenberger)
9. Exercise, Due 11 December, 2019

81. Find (without using a computer) the last two digits of 2^{1000}.

Proof. First notice that $\gcd(2,25) = 1$, therefore, applying Euler's theorem yields

$$2^{\varphi(25)} \underset{\text{mod } 25}{\equiv} 1$$

.

Notice also that $\varphi(25) = 25 \cdot \left(1 - \frac{1}{5}\right) = 20$.

Therefore $2^{20} \underset{\text{mod } 25}{\equiv} 1$; which implies that $2^{1000} \underset{\text{mod } 25}{\equiv} 1$.

Now, notice that $2^{1000} \underset{\text{mod } 4}{\equiv} 0$.

It follows from the Chinese Residue Theorem that there exists one unique solution modulo 100 for the following system of modulo equations.

$$x \underset{\text{mod } 25}{\equiv} 1$$
$$x \underset{\text{mod } 4}{\equiv} 0$$

From the previous equation system it follows that $x = 25 \cdot z_1 + 1$ and $x = 4 \cdot z_2$. Notice that $4 \cdot z_2 - 25 \cdot z_1 = 1$. Notice that $4 \cdot (-6) - 25(-1)$. This shows that $-24 = 76$ is the only solution for the equations modulo 100. Notice that 2^{1000} is also a solution. Therefore $2^{1000} \underset{\text{mod } 100}{\equiv} 76$. Therefore these are the last 2 numbers in decimal script of 2^{1000}. $\square$

82. Let a and b be two natural numbers such that $\gcd(a,b) = 1$. Prove that there exists a natural number c with $ac \underset{\text{mod } b}{\equiv} 1$. Find such c for $a = 55$ and $b = 42$.

Proof. Since $\gcd(a,b) = 1$, there is a linear combination $\alpha \cdot a + \beta \cdot b = 1$ such that $\alpha, \beta \in \mathbb{Z}$. Therefore $\alpha \cdot a = 1 + (-\beta) \cdot b$. This is the definition of $\alpha \cdot a \underset{\text{mod } b}{\equiv} 1$. Let $c := \alpha$.

For $a = 55$ and $b = 42$, we apply the Euclidian algorithm to express 1 as a linear combination of 55 and 42. We get that $1 = 13 \cdot 55 - 17 \cdot 42$. Therefore $c := 13$. $\square$

83. Let a and b be two natural numbers. Prove or disprove:

(a) If $\gcd(a,b)=1$ then $\gcd(a^2,ab,b^2)=1$.

Proof. Notice that since $\gcd(a,b)=1$ then $(a^2,ab)=a$ from using the prime power factorization of a and b. From the prime power factorization of a and b $\gcd(a,b^2)=1$. This shows that $\gcd(a^2,ab,b^2)$. $\square$

(b) If $a^2|b^3$ then $a|b$.
FALSE

Proof. Consider $a=2^3; b=2^2$, $a \nmid b$ but $a^3=2^6 \mid b^3=2^6$. $\square$

84. Prove that if a prime number p satisfies $\gcd(a,p-1)=1$, then for every integer b the congruence relation $x^a \underset{\text{mod } p}{\equiv} b$ admits a solution.

Proof. Notice that since p is a prime, then $\varphi(p)=p-1$. It follows from Euler's Theorem that for all $u \neq 0 \in \mathbb{Z}_p$, $u^{p-1}=1$.

Now notice that 0 trivially satisfies $x^a \underset{\text{mod} p}{\equiv} 0$.

Now consider the equation $x^n \underset{\text{mod } p}{\equiv} u$ for some $u \underset{\text{mod } p}{\not\equiv} 0$.

Notice that u is a unit in $\mathbb{Z}_p$, therefore u^z is well defined for all $z \in \mathbb{Z}_p$. Since $\gcd(a,p-1)=1$ there exists $\alpha,\beta \in \mathbb{Z}$ such that $\alpha\cdot(p-1)+\beta\cdot a=1$. It follows that in $\mathbb{Z}_p$:

$$u^{\alpha\cdot(p-1)+\beta\cdot a}=u$$
$$(u^{(p-1)})^\alpha\cdot(u^\beta)^a=u$$
$$(u^\beta)^a=u$$

Therefore u^β is a solution for equation $x^n \underset{\text{mod } p}{\equiv} u$. $\square$

85. Use the Chinese remainder theorem to solve the following system of congruence relations

$$3x \underset{\text{mod } 13}{\equiv} 12$$
$$5x \underset{\text{mod } 22}{\equiv} 7$$
$$4x \underset{\text{mod } 14}{\equiv} 6$$

Proof. Notice that this system of equations can be reduced to

$$x \underset{\text{mod } 13}{\equiv} 4$$
$$x \underset{\text{mod } 22}{\equiv} -3$$

$$x \underset{\text{mod } 7}{\equiv} 5$$

Since both 3 and 5 are units modulo 13 and 22 respectively. Notice that $4x \underset{\text{mod } 14}{\equiv} 6$ is equivalent to $4 \cdot x + \alpha \cdot 14 = 6$ for some $\alpha \in \mathbb{Z}$. Therefore $2 \cdot x + \alpha \cdot 7 = 3$, this is equivalent to $2 \cdot x \underset{\text{mod } 7}{\equiv} 3$ which in turn is equivalent to $x \underset{\text{mod } 7}{\equiv} 5$.

Now we can proceed to apply the Chinese Remainder Theorem.

We need to find an x_1 that solves $154 \cdot x_1 \underset{\text{mod } 13}{\equiv} 4$, which is equivalent to $-2 \cdot x_1 \underset{\text{mod } 13}{\equiv} 4$. Therefore $x_1 = -2$.

Now we proceed to find a solution for $91 \cdot x_2 \underset{\text{mod } 22}{\equiv} -3$. This is equivalent to finding a solution for $3 \cdot x_2 \underset{\text{mod } 22}{\equiv} -3$. Notice that $x_2 = -1$ is a solution.

At last we find a solution for $286 \cdot x_3 \underset{\text{mod } 7}{\equiv} 5$ which is equivalent to finding a solution for $6 \cdot x_3 \underset{\text{mod } 7}{\equiv} 5$ which in turn is equivalent to $-1 \cdot x_3 \underset{\text{mod } 7}{\equiv} -2$. Therefore $x_3 = 2$ is a solution.

We proceed to build the global solution by considering $7 \cdot 22 \cdot -2 + 13 \cdot 7 \cdot -1 + 13 \cdot 22 \cdot 2 = 173$ □

In the next three exercises λ will denote the Carmichael function and φ Euler's totient function.

86. Compute $\lambda(49392)$ and $\varphi(49392)$

Proof. We begin by obtaining the prime factorization of $z := 49392 = 2^4 \cdot 3^2 \cdot 7^3$ via the Sieve of Eratostenes.

Since $\varphi(a, b) = \varphi(a) \cdot \varphi(b)$ for relatively prime a, b. Then $\varphi(z) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(7^3)$.

Recall that

$$\varphi(p^r) = p^{r-1}(p-1)$$

Therefore $\varphi(2^4) = 2^3$, $\varphi(3^2) = 3 \cdot 2$, $\varphi(7^3) = 7^2 \cdot 2 \cdot 3$.

It follows that $\varphi(z) = 2^5 \cdot 3^2 \cdot 7^2$.

Notice that $\lambda(z) = \text{lcm}[\lambda(2^4), \lambda(3^2), \lambda(7^3)]$.

Recall that

$$\lambda(1) = 1; \lambda(2) = 1; \lambda(4) = 2$$

$$\lambda(2^e) = 2^{e-2} \text{ for } e \geq 3$$

$$\lambda(p^e) = p^{e-1}(p-1) \text{ for } p \in \mathbb{P}; p \neq 2$$

Therefore $\lambda(2^4) = 2^2$; $\lambda(3^2) = 3 \cdot 2$; $\lambda(7^3) = 7^2 \cdot 3 \cdot 2$.

$\lambda(z) = \text{lcm}[2^2, 2 \cdot 3, 2 \cdot 3 \cdot 7^2] = 2^2 \cdot 3 \cdot 7^2$

$\varphi(z) = 2^5 \cdot 3^2 \cdot 7^2$; $\lambda(z) = 2^2 \cdot 3 \cdot 7^2$ □

87. Prove that for all $m, n \in \mathbb{N}^+$, the following identity holds:

$$\varphi(m \cdot n) = \varphi(m)\varphi(n)\frac{\gcd(m,n)}{\varphi(\gcd(m,n))}$$

.

Proof. Let us recall that if $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is the prime power factorization of n, then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$.

Let $p_1, \dots, p_r$ be the prime divisors of m that don't divide n, $q_1, \dots, q_s$ the prime divisors of n that don't divide m, and $r_1, \dots, r_t$, the common prime divisors of m and n.

Let

$$P := \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

$$Q := \prod_{i=1}^{s}\left(1 - \frac{1}{q_i}\right)$$

$$R := \prod_{i=1}^{t}\left(1 - \frac{1}{r_i}\right)$$

It follows that $\varphi(m) = m \cdot P \cdot R$, $\varphi(n) = n \cdot Q \cdot R$, and $\varphi(m \cdot n) = m \cdot n \cdot P \cdot Q \cdot R = \dfrac{m \cdot Q \cdot R \cdot n \cdot Q \cdot R}{R} = \dfrac{\varphi(m) \cdot \varphi(n)}{R}$.

Since $\gcd(m,n)$ is a common divisor, then the prime power factorization of $\gcd(m,n)$ is given by $r_1, \dots, r_t$. it follows that $\varphi(\gcd(m,n)) = \gcd(m,n) \cdot R$. Therefore $R = \dfrac{\varphi(\gcd(m,n))}{\gcd(m,n)}$

Therefore $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \dfrac{\gcd(m,n)}{\varphi(\gcd(m,n))}$. ☐

88. Show that $m|n$ implies $\lambda(m)|\lambda(n)$.

Hint: first prove that

$$a_i | b_i \text{ for } i = 1, \dots, k \Longrightarrow \operatorname{lcm}(a_1, a_2, \dots, a_k) \mid \operatorname{lcm}(b_1, b_2, \dots, b_k)$$

.

Proof. We will first prove the hint.

Consider the $S = \{p_1, \dots, p_m\}$ the set of primes that divide some b_i with $i \in \{1, \dots, k\}$. Let $a_{i,j}$ be the power of p_j in the prime power factorization of a_i, and $a_{i,j}$ be defined in the same way for b_i.

Notice that the $\operatorname{lcm}(b_1, \ldots, b_k) = \prod_{j=1}^{m} p_i^{max_i b_{i,j}}$.

Likewise $\operatorname{lcm}(a_1, \ldots, a_k) = \prod_{j=1}^{m} p_i^{max_i a_{i,j}}$.

Notice that since each $a_i | b_i$, then for each i, $a_{i,j} \leq b_{i,j}$. Therefore $max_i a_{i,j} \leq max_i b_{i,j}$.

Therefore $\operatorname{lcm}(a_1, \ldots, a_k) \mid \operatorname{lcm}(b_1, \ldots, b_k)$

Now consider $m = p_1^{m_1} \ldots p_k^{m_k}$ and $n = p_1^{n_1} \ldots p_k^{n_k}$

Since $m \mid n$ it follows that each $m_i \leq n_i$.

Recall that $\lambda \left(\prod_{i=1}^{k} p_i^{e_i} \right) = \operatorname{lcm}(\lambda(p_1^{e_1}), \ldots, \lambda(p_k^{e_k}))$

Therefore $\lambda(m) = \operatorname{lcm}(\lambda(p_1^{m_1}), \ldots, \lambda(p_k^{m_k}))$ and $\lambda(n) = \operatorname{lcm}(\lambda(p_1^{n_1}), \ldots, \lambda(p_k^{n_k}))$

Also recall that

$$\lambda(1) = 1; \lambda(2) = 1; \lambda(4) = 2$$

$$\lambda(2^e) = 2^{e-2} \text{ for } e \geq 3$$

$$\lambda(p^e) = p^{e-1}(p-1) \text{ for } p \in \mathbb{P}; p \neq 2$$

Also since each $m_i \leq n_i$, then it follows that $\lambda(p_i^{m_i}) \mid \lambda(p_i^{n_i})$.

Applying the proof of the hint yields that

$$\lambda(m) = \operatorname{lcm}(\lambda(p_1^{m_1}), \ldots, \lambda(p_k^{m_k})) \mid \lambda(n) = \operatorname{lcm}(\lambda(p_1^{n_1}), \ldots, \lambda(p_k^{n_k}))$$

□

89. Let $(n, e) = (3233, 49)$ be a public RSA key. Compute the associated decryption key d.

Proof. The key is noting that $3233 = 53 \cdot 61$. Let's consider $\operatorname{lcm}(52 = 2^2 \cdot 13, 60 = 2^2 \cdot 3 \cdot 5) = 2^2 \cdot 3 \cdot 5 \cdot 13 = 780$.

In order to find the decription key d, we apply the Euclidian algorithm to find a linear combination of 780 and 49 that is equal to 1.

This leads to

$$12 \cdot 780 - 191 \cdot 49 = 1$$

.

Therefore the public key $d = -191 = 589$. A quick sanity check verifies that indeed $589 \cdot 49 \underset{\text{mod } 780}{\equiv} 1$. □

90. Consider the encoding of a string s, parsed into blocks of two letters, via the mapping

$$A \mapsto 01, \quad B \mapsto 02, \quad \ldots, \quad Z \mapsto 26$$

.

Thus s is encoded into a sequence of integers, one for each block and each with at most four digits. For example, $s = \text{BAZC} \mapsto (201, 2603)$. Each element of the list is then further encoded using the public RSA key of exercise 89.

The sequence $(2701, 2593, 371, 1002)$ was encoded via the two steps described above.

Decode it, i.e. find the original string.

For this purpose we help ourselves with the following python snippet.

```
def modp (n,m,k):
    ans = 1
    for i in range(m):
        ans = (ans*n)%k
    return ans

def letter (n):
    print chr(n+96)
```

Since we already cracked the key d in the previous exercise, then we only need to input the blocks and raise them to the 589^{th} power modulo 3233.

This yields the following blocks $(0315, 1316, 2120, 0518)$ which is decifered as 'computer'.