Yinghua Wu

Solutions to Problem Set 3

Problem 9: Linear Diophantine Equations (3.13.1)

(a) This problem can be directly solved by using the extended Euclidean algorithm or just the basic Euclidean algorithm as follows:

$$\begin{aligned} 101 &= 17 * 5 + 16 \\ 17 &= 16 * 1 + 1 \end{aligned}$$

So $\gcd(101, 17) = 1$, and $17x + 101y = 1$ have integer solutions. We rewrite the above equations as

$$\begin{aligned} 16 &= 101 - 17 * 5 \\ 1 &= 17 - 16 \end{aligned}$$

from which we obtain $1 = 17 - 16 = 17 - (101 - 17 * 5) = 17 * 6 - 101$. So $x = 6$ and $y = -1$.

(b) From (a), we immediately know $17^{-1} \pmod{101} \equiv 6$.

Problem 10: Euclidean Algorithm (3.13.5)

(a) Using Euclidean algorithm, we have

$$\begin{aligned} 4883 &= 4369 * 1 + 514 \\ 4369 &= 514 * 8 + 257 \\ 514 &= 257 * 2 \end{aligned}$$

So $\gcd(4883, 4369) = 257$.

(b) From (a), fortunately 257 is a prime itself. So $4883 = 257 * 19$ and $4369 = 257 * 17$.

Problem 11: Quadratic Diophantine Equation (3.13.8)

The conclusion of $7(a)$ needs to be proved first if used in this problem, and that p is a prime is definitely a necessary condition which must be used in the proof.

Now we prove $7(a)$ first.

$7(a)$ Let p be prime. Suppose a and b are integers such that $ab \equiv 0 \pmod p$. Show that either $a \equiv 0$ or $b \equiv 0 \pmod p$.

Proof: Since $ab \equiv 0 \pmod p$, we have $p|ab$. Since p is prime, we obtain that either $p|a$ or $p|b$ holds and is also necessary for $p|ab$. So either $a \equiv 0$ or $b \equiv 0 \pmod p$ holds and is necessary and also obviously sufficient.

Coming back to our problem, we know that p is a prime and $x^2 \equiv 1 \pmod p$. We rewrite the above equation to $x^2 - 1 \equiv (x+1)(x-1) \equiv 0 \pmod p$. From the conclusion of $7(a)$, we get that either $x + 1 \equiv 0 \pmod p$ or $x - 1 \equiv 0 \pmod p$ holds and is necessary and sufficient for $(x+1)(x-1) \equiv 0 \pmod p$. Since $p \geq 3$, $x \equiv \pm 1 \pmod p$ are two different solutions and also the only solutions because they are necessary and sufficient for the problem.

Problem 12: Chinese Remainder Theorem (3.13.10)

This problem can be formatted into a remainder problem as the following:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5, \end{aligned}$$

in which x is the number of people.

Following the procedure of Exercise 24, we can solve the above problem as the following:

$$z_1 = 4 * 5 = 20, z_2 = 3 * 5 = 15, z_3 = 3 * 4 = 12,$$

and

$$y_1 \equiv z_1^{-1} \equiv 2 \pmod 3), y_2 \equiv z_2^{-1} \equiv 3 \pmod 4), y_3 \equiv z_3^{-1} \equiv 3 \pmod 5).$$

So we have $x = 1 * y_1 * z_1 + 2 * y_2 * z_2 + 3 * y_3 * z_3 = 238$. To get the smallest solution, we obtain $238 \equiv 58 \pmod{3 * 4 * 5}$, and the next solution is $58 + (3 * 4 * 5) = 118$.

Problem 13: RSA Encryption (6.8.2)

(a) Since $\phi(n) = (5-1)*(11-1) = 40$, we just simply calculate the inverse of e as $d \equiv e^{-1} \equiv 27 \pmod{\phi(n)}$ using extended Euclidean algorithm.

(b) We try to prove a more general case that if $c \equiv m^e \pmod n$, then $m \equiv c^d \equiv m^{ed} \pmod n$ in which $\gcd(m, n) = 1$. From (a), we know that $ed \equiv 1 \pmod{\phi(n)}$, so $ed = 1 + k * \phi(n)$, in which k is an integer. So we obtain that $m^{ed} \equiv m^{1+k*\phi(n)} \equiv m * m^{k*\phi(n)} \pmod n$. From Euler's theorem, we know that if $\gcd(m, n) = 1$, $m^{\phi(n)} \equiv 1 \pmod n$. So $m^{k*\phi(n)} \equiv 1 \pmod n$ and $m * m^{k*\phi(n)} \equiv m \pmod n$ and the proposition is proved.

Problem 14: RSA Attack (6.8.3)

We know $c = 75$, $e = 3$ and $n = 437$, so just try possible plaintext 8 and 9. And we get $8^3 \equiv 75 \pmod{437}$, so 8 is the plaintext.

Problem 15: RSA Decryption Exponent (6.8.5)

Assume $e \neq 0$ and $e \neq p-1$ since it is 'suitably chosen', otherwise, y will be a constant independent of x and then there is no hope for us to recover x. Now we need to find d so that $y^d \equiv x^{ed} \equiv x \pmod p$. According to Fermat's Little Theorem, we know that if $ed \equiv 1 \pmod{(p-1)}$, then $x^{ed} \equiv x \pmod p$ which satisfies our requirement. So we can let $d = e^{-1} \pmod{(p-1)}$ if $e^{-1} \pmod{(p-1)}$ does exist.

Problem 16: Factoring (6.8.12)

From the problem, we have

$$\begin{aligned} 516107^2 &\equiv 7 \pmod n \\ 187722^2 &\equiv 2^2 * 7 \pmod n \end{aligned}$$

So we obtain $(516107 * 187722)^2 \equiv (2 * 7)^2 \pmod n$ by multiplying the above two equations. $516107 * 187722 \equiv 289038 \not\equiv \pm 14 \pmod n$, so if we compute $\gcd(289038 - 14, n)$, we can get a non-trivial factor. Using Euclidean algorithm, we have $\gcd(289038, 642401) = 1129$. So $n = 1129 * 569$, in which both factors are prime.