17/20

MAT246 HW5 Rui Qiu 999292509

#1.

(a). Proof:

By definition we say $g_1 = \gcd(a,b,c)$ with $g_1|a$, $g_1|b$, $g_1|c$.

Similarly say $g_2 = \gcd(\gcd(a,b), c)$ with

$$g_2 | \gcd(a,b),\ g_2|c$$

Since $g_2|\gcd(a,b)$

Then $g_2|a$, $g_2|b$

Since g_1 is the greatest common divisor of a,b,c

g_2 is a common divisor of a,b,c.

Then $g_2|g_1$.

Similarly Since g_2 is the greatest common divisor of $\gcd(a,b), c$

g_1 is a common divisor of $\gcd(a,b)$

(Why? Because $g_1|a$, $g_1|b$)

Then $g_1|g_2$

Therefore $g_1 = g_2$

Thus $\gcd(a,b,c) = \gcd(\gcd(a,b),c)$ ∎

(b). Proof:

Let $\gcd(a,b,c) = \gcd(\gcd(a,b),c) = d$

~~$\gcd(a,b) = m$~~

Then $ax+by+cz = d$

~~Suppose~~

Since $d|\gcd(a,b,c)$, using the Euclidean algorithm

there exist two integers x_0, y_0 such that

$$ax_0 + by_0 = \gcd(a,b)$$

Similary, there exist two integers w_0, z_0 such that

$$\gcd(a,b)w_0 + cz_0 = d$$

Then $d = \gcd(a,b)w_0 + cz_0$

$$= (ax_0 + by_0)w_0 + cz_0$$

$$= a(x_0w_0) + b(y_0w_0) + cz_0 \quad \text{with } x_0w_0, y_0w_0, z_0 \in \mathbb{Z}$$

Therefore it has an integer solution. ∎

#2.

Solution: We can find $6^{100} \bmod 7$ first instead of $6^{100} \bmod 14$
Since $\gcd(6,7)=1$, $\gcd(6,14)\neq 1$.

Since $6^{\varphi(7)} \equiv 6^6 \bmod 7 \equiv 1 \bmod 7$
then $6^{100} \equiv 6^{6\times 16+4} \equiv (6^6)^{16} \cdot 6^4 \bmod 7$
$\equiv 1^{16} \cdot (36)^2 \bmod 7$
$\equiv 1^2 \bmod 7$
$\equiv 1 \bmod 7$

2/5

Then $6^{100} \equiv 1 \bmod 7 \equiv 1+7 \bmod 7$
$\equiv 8 \bmod 7$

Therefore $6^{100} \bmod 14 \equiv 8 \bmod 14$. ← What is this magic?

MAT246 HW5 Rui Qiu 999292509

#3.

Proof: Since $m \equiv 1 \mod \varphi(n)$

Then $m-1 = k\varphi(n)$ for some $k \in \mathbb{Z}$

By Euler's Theorem, $(a,n)=1$.

$$a^{\varphi(n)} \equiv 1 \mod n$$

Then $a^{m-1} \equiv a^{\varphi(n)\cdot k} \equiv (a^{\varphi(n)})^k \mod n$

$$\equiv 1^k \mod n$$
$$\equiv 1 \mod n$$

Therefore $a^{m-1} = n \cdot r + 1$ for some $r \in \mathbb{Z}$

Both sides time a we get:

$$a^m = ar \cdot n + a$$

Hence $a^m \equiv a \mod n$ ∎

Textbook problems:

Pg. 49.

#1. RSA, $p=5$, $q=7$, $E=5$.

Verify $D=5$ is a decoder.

encoded message is 17. what is decoded message?

Solution: We need a D s.t. $DE \equiv 1 \mod \varphi(N)$

Then take $D=5$

$$5\times 5 \equiv 25 \equiv 1 \mod \varphi(5\times 7)$$
$$\equiv 1 \mod 24$$

Verified. $D=5$ is a decoder. ✓

For $R=17$

$R^D = 17^5 \bmod 35$

$\equiv (17^2)^2 \cdot 17 \bmod 35$

$\equiv (9)^2 \cdot 17 \bmod 35$

$\equiv 11 \cdot 17 \bmod 35$

$\equiv 12 \bmod 35$

So the decoded message is 12.

Check that $12^5 \bmod 35 \equiv 17 \bmod 35$

#2. RSA, $N=21$, $E=5$.

(a). Encrypt the message $M=7$

Solution: $M^E \equiv R \pmod N$

$7^5 \equiv (7^2)^2 \cdot 7 \bmod 21$

$= (7)^2 \cdot 7 \bmod 21$

$\equiv 7 \cdot 7 \bmod 21$

$= 7 \bmod 21$

so $R=7$

The sending message should be 7.

(b) Verify $D=5$ is a decoder.

Solution: $N = p \cdot q \Rightarrow 35 = 5 \times 7$ which is the prime factorization of N

So $\varphi(N) = (p-1) \times (q-1) = 4 \times 6 = 24$

We have $E=5$, to check whether D is a decoder.

$DE \bmod \varphi(N)$

$\equiv 5 \times 5 \bmod 4 \times 6$

$\equiv 25 \bmod 24$

$\equiv 1 \bmod 24$

Thus $D=5$ is a decoder in this RSA system.

MAT246 HW5 Rui Qiu 999292509

(C). Decrypt the encrypted form of the message.

Solution: what we know here is $R=7, N=21, E=5, D=5$ which is verified in (b).
Want to know M

$$\begin{aligned} R^D &\equiv 7^5 \bmod 21 \\ &\equiv (7^2)^2 \cdot 7 \bmod 21 \\ &\equiv (7)^2 \cdot 7 \bmod 21 \\ &\equiv 7 \cdot 7 \bmod 21 \\ &\equiv 7 \bmod 21 \end{aligned}$$

Hence $M=7$, the decoded form is 7.