Sample Quiz — Solutions

1. Find $\gcd(10^{20}, 84)$.

Solution $10^{20} = 2^{20} \times 5^{20}$ and $84 = 2^2 \times 3 \times 7$, so $\gcd(10^{20}, 84) = 2^2 = 4$.

2. Find the smallest prime which divides 123456789123456789.

Solution The sum of the digits of this number is 90, so it is divisible by 3; and it is clearly not even, so the answer is 3.

3. Find which element of $\{1, 2, \cdots, 58\}$ is inverse to 17 modulo 59.

Solution Since $7 \times 17 = 119 \equiv 1 \pmod{59}$, 7 is an answer, necessarily the unique answer. This could be found using the extended Euclidean Algorithm, for instance.

4. Find the order of 5 modulo 31.

Solution Since $5^3 = 125 \equiv 1 \pmod{31}$, and obviously $5^2 \not\equiv 1 \pmod{31}$, the order of 5 modulo 31 is 3.

5. Find the residue of 3^{1010} modulo 7.

Solution The order of 3 modulo 7 is 6 (in fact, all we need to know is that it divides 6, which holds by Fermat's Little Theorem). Since $1010 \equiv 2 \pmod{6}$, $3^{1010} \equiv 3^2 \equiv 2 \pmod{7}$. So the answer is 2.

6. Find the unique $x \in \{0, 1, 2, \cdots, 194\}$ such that $x \equiv 3 \pmod{13}$ and $x \equiv 2 \pmod{15}$.

Solution Substituting $x = 3 + 13k$ into the second congruence and simplifying, it becomes $13k \equiv -1 \pmod{15}$. An inverse of 13 modulo 15 is 7, so this is equivalent to $k \equiv -7 \equiv 8 \pmod{15}$. Substituting $k = 8 + 15\ell$ into the expression for x we get the general solution $x = 107 + 195\ell$. So 107 is the unique solution in $\{0, 1, 2, \cdots, 194\}$.

7. Find the residue of 2^{1010} modulo 111.

Solution The prime factorization of 111 is 3×37, so $\varphi(111) = 2 \times 36 = 72$. By the Euler–Fermat Theorem, $2^{72} \equiv 1 \pmod{111}$. Since $1010 \equiv 2 \pmod{72}$, we have $2^{1010} \equiv 2^2 \pmod{111}$, so the answer is 4. An alternative is to find the residue of 2^{1010} modulo the primes 3 and 37 separately, and then combine that information by solving a system of simultaneous congruences.

8. Find $\sigma(640)$, the sum of the positive integer divisors of 640.

Solution Since $640 = 2^7 \times 5$, we have $\sigma(640) = \sigma(2^7)\sigma(5) = (2^8 - 1)(1 + 5) = 1530$.

9. What is the smallest positive integer with exactly 10 positive divisors?

Solution If $n = p_1^{k_1} \cdots p_r^{k_r}$, then the number of divisors $\tau(n) = (k_1 + 1) \cdots (k_r + 1)$. The only ways to write 10 as a product of integers ≥ 2 are 10 and 5×2, so for $\tau(n) = 10$ we must have either $n = p_1^9$ or $n = p_1^4 p_2$. The smallest number of the first form is $2^9 = 512$ and the smallest number of the second form is $2^4 3 = 48$, so the answer is 48.

10. If a simple substitution cipher encrypts the word `SUGAR` as `JWZXD`, what is the decryption of `XDZWJ`?

Solution A simple substitution cipher replaces each particular letter of the alphabet with the same substitute letter, no matter where in the message it is. In this cipher `S` is replaced by `J`, `U` by `W`, and so on. So the decryption of `XDZWJ` is `ARGUS`.

11. What would be the output of the following MAGMA commands?


```
> V:=VigenereCryptosystem(3);
> encipheringkey:=V!"BAY";
> Enciphering(encipheringkey,Encoding(V,"HOTEL"));
```

Solution These commands tell MAGMA to use a Vigenere cipher with keyword `BAY` to encipher the word `HOTEL`. Since the first letter of the keyword is `B` which follows `A` in the alphabet, the first and fourth letters should be moved one letter further on in the alphabet; since the second letter of the keyword is `A`, the second and fifth letters should be left unchanged; since the third letter of the keyword is `Y` which is two letters before `A` (working mod 26), the third letter should be moved two letters back in the alphabet. So the output will be `IORFL`.

12. Suppose you are given two long ciphertexts `sct1` and `sct2` and told that one of them is some ordinary English text enciphered with a block transposition cipher and the other is the same English text enciphered with a Vigenere cipher. If you see the following MAGMA code, which one was (probably) enciphered using the block transposition cipher?

```
> CoincidenceIndex(sct1);
0.065201231214704805740688281507 1
> CoincidenceIndex(sct2);
0.041587978794878087462142783659 4
```

Solution Transposition ciphers do not change the coincidence index, since they just permute the letters of the plaintext, whereas Vigenere ciphers tend to lower it because they even out the frequency distribution of letters. So we can be fairly certain that `sct1` is the ciphertext which was enciphered using the block transposition cipher.

13. If an RSA cryptosystem has public key $(22, 3)$, what is the decryption exponent?

Solution The decryption exponent is the inverse of 3 modulo $\varphi(22) = 10$, which is 7.

14. Suppose that an RSA cryptosystem has a public key of $(33, 3)$. Encrypt the message $[4, 6]$.

Solution To encrypt, we raise each letter of the plaintext to the power 3 and reduce modulo 33. Since $4^3 = 64 \equiv 31 \pmod{33}$ and $6^3 = 6^2 \times 6 \equiv 3 \times 6 = 18 \pmod{33}$, the answer is $[31, 18]$.

15. What would be the output of the following MAGMA commands?

```
> p:=NextPrime(100);
> 6^p mod p;
```

Solution These command tell MAGMA to define p to be the next prime after 100 (actually 101, but we don't need to know that) and then calculate the residue of 6^p modulo p. By Fermat's Little Theorem, the answer is 6.