QuizA — Solutions

1. Find the order of 11 modulo 43.

Solution We know that the order of 11 modulo 43 must divide 42 by Fermat's Little Theorem, which reduces the number of residues that we need to consider. Since $11^7 \equiv 1 \pmod{43}$, and for any proper divisor d of 7 we check that $11^d \not\equiv 1 \pmod{43}$, the order of 11 modulo 43 must be 7.

2. If an RSA cryptosystem has modulus 55 and a decryption exponent 23, what is the encryption exponent?

Solution The encryption exponent is the inverse of 23 modulo $\varphi(55) = 40$, which is 7.

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

```
> CoincidenceIndex(sct1);
0.043287808746214278365941587978 79
> CoincidenceIndex(sct2);
0.064588057406882815071520123121 4
```

Solution Simple substitution ciphers do not change the coincidence index, since they just permute the frequencies of letters around, whereas Vigenère 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 Vigen'ere cipher.

4. Find the number of positive integer divisors of 320.

Solution Since $320 = 2^6 \times 5^1$, we have $\tau(320) = (6+1)(1+1) = 14$.

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

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

Solution These commands tell MAGMA to use a Vigenere cipher with keyword `BED` to encipher the word `CORE`. 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 `E`, the second letter should be moved four letters further on in the alphabet; since the third letter of the keyword is `D`, the third letter should be moved three letters further on in the alphabet. So the output will be `DSUF`.

6. Find the unique $x \in \{0, 1, 2, \cdots, 139\}$ such that $x \equiv 5 \pmod{7}$ and $x \equiv 3 \pmod{20}$.

Solution Firstly find integer s and t such that $1 = s \cdot 7 + t \cdot 20$. One can find that $1 = 3 \cdot 7 - \cdot 20$. Then $x \equiv 3 \cdot 3 \cdot 7 - 5 \cdot 20 \equiv -37 \pmod{140}$ Finally, we need to add 140 to the answer to get 103.

7. Find which element of $\{1, 2, \cdots, 40\}$ is inverse to 28 modulo 41.

Solution The Euclidean Algorithm applied to 41 and 28 gives

$$41 = 28 + 13$$
$$28 = 2 \times 13 + 2$$
$$13 = 6 \times 2 + 1$$

Rearranging this information (or using the extended Euclidean algorithm), we get that $1 = 13 \times 41 - 19 \times 28$. So -19 is an inverse of 28 modulo 41, and the desired answer is 22.

8. Suppose that an RSA cryptosystem has a public key of $(55, 3)$. Encrypt the message $[2, 4]$.

Solution To encrypt, we raise each letter of the plaintext to the power 3 and reduce modulo 55. Since $4^3 = 64 \equiv 9 \pmod{55}$, the answer is $[8, 9]$.

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

```
> p:=NextPrime(1024);
> n:=p*p*p;
> EulerPhi(n) mod p;
```

Solution These commands tell MAGMA to let p be the next prime after 1000 (which is actually 1031, but we don't need to know that), then let $n = p^3$ and find the residue of $\varphi(n)$ modulo p. Since $\varphi(p^3) = p^2(p-1)$, the answer is 0.

10. Find the residue of 3^{4804} modulo 65.

Solution The prime factorization of 65 is 5×13, so $\varphi(65) = 4 \times 12 = 48$. Since $4804 \equiv 4 \pmod{48}$, we have $3^{4804} \equiv 3^4 = 81 \pmod{65}$, so the answer is $81 - 65 = 16$.

An alternative is to find the residue of 3^{4804} modulo the primes 5 and 13 separately, and then combine that information by solving a system of simultaneous congruences.

11. If a transposition cipher encrypts the word `MELON` as `ENOML`, what is the **decryption** of `RENCO`?

Solution A transposition cipher permutes the letters of the plaintext according to some fixed permutation. In this case we see that the first letter goes to fourth place, the second letter goes to first place, the third letter goes to fifth place, fourth letter to third place and fifth letter to second place. So the decryption of `RENCO` is `CRONE`.

12. Find $\sigma(2291)$, the sum of all the positive integer divisors of 2291.

Solution Since 2291 has prime factorization 29×79, its positive divisors are $1, 29, 79, 2291$. So the answer is 2400.

13. Find $\gcd(4^{100} - 1, 21)$.

Solution

Prime factors of 21 are 3 and 7. So we check the divisibility of $4^{100} - 1$ by each of those factors independently. $3 - 1$ definitely divides 100 therefore, by Fermat Little Theorem, $3 \mid 4^{100} - 1$. Also, $4^6 \equiv 1 \pmod{7}$ and therefore $4^{100} \equiv 4^4 \not\equiv 1 \pmod{7}$. Therefore the final answer is 3.

Alternatively, one can use the Euler-Fermat theorem straight away.

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

```
> n:=125;
> Factorial(n-1) mod (n^8);
```

Solution These commands tell MAGMA to find the residue of 124! modulo $125^8 = 5^{24}$. Since 24 of the terms in 124! are multiples of 5, 124! is divisible by 5^{24}. Therefore the answer is 0.

15. Function f is defined as follows:

$$f(n) := \sum_{d \mid n} \mu(d) \cdot d^2,$$

where $\mu(n)$ is the Möbius function. Compute $f(192)$.

Solution $\mu(d)$ and d^2 are both multiplicative. Therefore their product and in turn $f(n)$ is multiplicative too. The prime factorization of 192 is $2^6 \cdot 3^1$.

Hence we have

$$f(192) = f(64) \cdot f(3) = (1 - 2^2)(1 - 3^2) = 24.$$

QuizB — Solutions

1. Find the order of 2 modulo 23.

Solution We know that the order of 2 modulo 23 must divide 22 by Fermat's Little Theorem, which reduces the number of residues that we need to consider. Since $2^{11} \equiv 1 \pmod{23}$, and for any proper divisor d of 11 we check that $2^d \not\equiv 1 \pmod{23}$, the order of 2 modulo 23 must be 11.

2. If an RSA cryptosystem has modulus 77 and a decryption exponent 43, what is the encryption exponent?

Solution The encryption exponent is the inverse of 43 modulo $\varphi(77) = 60$, which is 7.

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

```
> CoincidenceIndex(sct1);
0.043287808746214278365941587978 79
> CoincidenceIndex(sct2);
0.064588057406882815071520123121 4
```

Solution Simple substitution ciphers do not change the coincidence index, since they just permute the frequencies of letters around, whereas Vigenère 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 Vigen'ere cipher.

4. Find the number of positive integer divisors of 200.

Solution Since $200 = 2^3 \times 5^2$, we have $\tau(200) = (3 + 1)(2 + 1) = 12$.

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

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

Solution These commands tell MAGMA to use a Vigenere cipher with keyword `BED` to encipher the word `CORE`. 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 `E`, the second letter should be moved four letters further on in the alphabet; since the third letter of the keyword is `D`, the third letter should be moved three letters further on in the alphabet. So the output will be `DSUF`.

6. Find the unique $x \in \{0, 1, 2, \cdots, 351\}$ such that $x \equiv 5 \pmod{11}$ and $x \equiv 2 \pmod{32}$.

Solution Firstly find integer s and t such that $1 = s \cdot 11 + t \cdot 32$. One can find that $1 = 3 \cdot 11 - \cdot 32$. Then $x \equiv 2 \cdot 3 \cdot 11 - 5 \cdot 32 \equiv -94 \pmod{352}$ Finally, we need to add 352 to the answer to get 258.

7. Find which element of $\{1, 2, \cdots, 36\}$ is inverse to 30 modulo 37.

Solution The Euclidean Algorithm applied to 37 and 30 gives

$$37 = 30 + 7$$
$$30 = 4 \times 7 + 2$$
$$7 = 3 \times 2 + 1$$

Rearranging this information (or using the extended Euclidean algorithm), we get that $1 = 13 \times 37 - 16 \times 30$. So -16 is an inverse of 30 modulo 37, and the desired answer is 21.

8. Suppose that an RSA cryptosystem has a public key of $(51, 3)$. Encrypt the message $[2, 4]$.

Solution To encrypt, we raise each letter of the plaintext to the power 3 and reduce modulo 51. Since $4^3 = 64 \equiv 13 \pmod{51}$, the answer is $[8, 13]$.

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

```
> p:=NextPrime(1024);
> n:=p*p*p;
> EulerPhi(n) mod p;
```

Solution These commands tell MAGMA to let p be the next prime after 1000 (which is actually 1031, but we don't need to know that), then let $n = p^3$ and find the residue of $\varphi(n)$ modulo p. Since $\varphi(p^3) = p^2(p-1)$, the answer is 0.

10. Find the residue of 3^{4004} modulo 55.

Solution The prime factorization of 55 is 5×11, so $\varphi(55) = 4 \times 10 = 40$. Since $4004 \equiv 4 \pmod{40}$, we have $3^{4004} \equiv 3^4 = 81 \pmod{55}$, so the answer is $81 - 55 = 26$.

An alternative is to find the residue of 3^{4004} modulo the primes 5 and 11 separately, and then combine that information by solving a system of simultaneous congruences.

11. If a transposition cipher encrypts the word `MELON` as `ENOML`, what is the **decryption** of `RENCO`?

Solution A transposition cipher permutes the letters of the plaintext according to some fixed permutation. In this case we see that the first letter goes to fourth place, the second letter goes to first place, the third letter goes to fifth place, fourth letter to third place and fifth letter to second place. So the decryption of `RENCO` is `CRONE`.

12. Find $\sigma(2231)$, the sum of all the positive integer divisors of 2231.

Solution Since 2231 has prime factorization 23×97, its positive divisors are $1, 23, 97, 2231$. So the answer is 2352.

13. Find $\gcd(2^{100} - 1, 35)$.

Solution

Prime factors of 35 are 5 and 7. So we check the divisibility of $2^{100} - 1$ by each of those factors independently. $5 - 1$ definitely divides 100 therefore, by Fermat Little Theorem, $5 \mid 2^{100} - 1$. Also, $2^6 \equiv 1 \pmod{7}$ and therefore $2^{100} \equiv 2^4 \not\equiv 1 \pmod{7}$. Therefore the final answer is 5.

Alternatively, one can use the Euler-Fermat theorem straight away.

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

```
> n:=125;
> Factorial(n-1) mod (n^8);
```

Solution These commands tell MAGMA to find the residue of 124! modulo $125^8 = 5^{24}$. Since 24 of the terms in 124! are multiples of 5, 124! is divisible by 5^{24}. Therefore the answer is 0.

15. Function f is defined as follows:

$$f(n) := \sum_{d \mid n} \mu(d) \cdot d^2,$$

where $\mu(n)$ is the Möbius function. Compute $f(216)$.

Solution $\mu(d)$ and d^2 are both multiplicative. Therefore their product and in turn $f(n)$ is multiplicative too. The prime factorization of 216 is $2^3 \cdot 3^3$.

Hence we have

$$f(216) = f(8) \cdot f(27) = (1 - 2^2)(1 - 3^2) = 24.$$

QuizC — Solutions

1. Find the order of 3 modulo 61.

Solution We know that the order of 3 modulo 61 must divide 60 by Fermat's Little Theorem, which reduces the number of residues that we need to consider. Since $3^{10} \equiv 1 \pmod{61}$, and for any proper divisor d of 10 we check that $3^d \not\equiv 1 \pmod{61}$, the order of 3 modulo 61 must be 10.

2. If an RSA cryptosystem has modulus 65 and a decryption exponent 29, what is the encryption exponent?

Solution The encryption exponent is the inverse of 29 modulo $\varphi(65) = 48$, which is 5.

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

```
> CoincidenceIndex(sct1);
0.043287808746214278365941587978 79
> CoincidenceIndex(sct2);
0.064588057406882815071520123121 4
```

Solution Simple substitution ciphers do not change the coincidence index, since they just permute the frequencies of letters around, whereas Vigenère 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 Vigen'ere cipher.

4. Find the number of positive integer divisors of 2000.

Solution Since $2000 = 2^4 \times 5^3$, we have $\tau(2000) = (4+1)(3+1) = 20$.

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

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

Solution These commands tell MAGMA to use a Vigenere cipher with keyword `BED` to encipher the word `CORE`. 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 `E`, the second letter should be moved four letters further on in the alphabet; since the third letter of the keyword is `D`, the third letter should be moved three letters further on in the alphabet. So the output will be `DSUF`.

6. Find the unique $x \in \{0, 1, 2, \cdots, 351\}$ such that $x \equiv 7 \pmod{11}$ and $x \equiv 5 \pmod{32}$.

Solution Firstly find integer s and t such that $1 = s \cdot 11 + t \cdot 32$. One can find that $1 = 3 \cdot 11 - \cdot 32$. Then $x \equiv 5 \cdot 3 \cdot 11 - 7 \cdot 32 \equiv -59 \pmod{352}$ Finally, we need to add 352 to the answer to get 293.

7. Find which element of $\{1, 2, \cdots, 42\}$ is inverse to 39 modulo 43.

Solution The Euclidean Algorithm applied to 43 and 39 gives

$$43 = 39 + 4$$
$$39 = 9 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$

Rearranging this information (or using the extended Euclidean algorithm), we get that $1 = 10 \times 43 - 11 \times 39$. So -11 is an inverse of 39 modulo 43, and the desired answer is 32.

8. Suppose that an RSA cryptosystem has a public key of $(33, 3)$. Encrypt the message $[2, 4]$.

Solution To encrypt, we raise each letter of the plaintext to the power 3 and reduce modulo 33. Since $4^3 = 64 \equiv 31 \pmod{33}$, the answer is $[8, 31]$.

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

```
> p:=NextPrime(1024);
> n:=p*p*p;
> EulerPhi(n) mod p;
```

Solution These commands tell MAGMA to let p be the next prime after 1000 (which is actually 1031, but we don't need to know that), then let $n = p^3$ and find the residue of $\varphi(n)$ modulo p. Since $\varphi(p^3) = p^2(p-1)$, the answer is 0.

10. Find the residue of 3^{4404} modulo 69.

Solution The prime factorization of 69 is 3×23, so $\varphi(69) = 2 \times 22 = 44$. Since $4404 \equiv 4 \pmod{44}$, we have $3^{4404} \equiv 3^4 = 81 \pmod{69}$, so the answer is $81 - 69 = 12$.

An alternative is to find the residue of 3^{4404} modulo the primes 3 and 23 separately, and then combine that information by solving a system of simultaneous congruences.

11. If a transposition cipher encrypts the word `MELON` as `ENOML`, what is the **decryption** of `RENCO`?

Solution A transposition cipher permutes the letters of the plaintext according to some fixed permutation. In this case we see that the first letter goes to fourth place, the second letter goes to first place, the third letter goes to fifth place, fourth letter to third place and fifth letter to second place. So the decryption of `RENCO` is `CRONE`.

12. Find $\sigma(2047)$, the sum of all the positive integer divisors of 2047.

Solution Since 2047 has prime factorization 23×89, its positive divisors are $1, 23, 89, 2047$. So the answer is 2160.

13. Find $\gcd(5^{100} - 1, 21)$.

Solution

Prime factors of 21 are 3 and 7. So we check the divisibility of $5^{100} - 1$ by each of those factors independently. $3 - 1$ definitely divides 100 therefore, by Fermat Little Theorem, $3 \mid 5^{100} - 1$. Also, $5^6 \equiv 1 \pmod{7}$ and therefore $5^{100} \equiv 5^4 \not\equiv 1 \pmod{7}$. Therefore the final answer is 3.

Alternatively, one can use the Euler-Fermat theorem straight away.

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

```
> n:=125;
> Factorial(n-1) mod (n^8);
```

Solution These commands tell MAGMA to find the residue of 124! modulo $125^8 = 5^{24}$. Since 24 of the terms in 124! are multiples of 5, 124! is divisible by 5^{24}. Therefore the answer is 0.

15. Function f is defined as follows:

$$f(n) := \sum_{d \mid n} \mu(d) \cdot d^2,$$

where $\mu(n)$ is the Möbius function. Compute $f(144)$.

Solution $\mu(d)$ and d^2 are both multiplicative. Therefore their product and in turn $f(n)$ is multiplicative too. The prime factorization of 144 is $2^4 \cdot 3^2$.

Hence we have

$$f(144) = f(16) \cdot f(9) = (1 - 2^2)(1 - 3^2) = 24.$$

QuizD — Solutions

1. Find the order of 3 modulo 41.

Solution We know that the order of 3 modulo 41 must divide 40 by Fermat's Little Theorem, which reduces the number of residues that we need to consider. Since $3^8 \equiv 1 \pmod{41}$, and for any proper divisor d of 8 we check that $3^d \not\equiv 1 \pmod{41}$, the order of 3 modulo 41 must be 8.

2. If an RSA cryptosystem has modulus 51 and a decryption exponent 23, what is the encryption exponent?

Solution The encryption exponent is the inverse of 23 modulo $\varphi(51) = 32$, which is 7.

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

```
> CoincidenceIndex(sct1);
0.043287808746214278365941587978 79
> CoincidenceIndex(sct2);
0.064588057406882815071520123121 4
```

Solution Simple substitution ciphers do not change the coincidence index, since they just permute the frequencies of letters around, whereas Vigenère 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 Vigen'ere cipher.

4. Find the number of positive integer divisors of 400.

Solution Since $400 = 2^4 \times 5^2$, we have $\tau(400) = (4+1)(2+1) = 15$.

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

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

Solution These commands tell MAGMA to use a Vigenere cipher with keyword `BED` to encipher the word `CORE`. 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 `E`, the second letter should be moved four letters further on in the alphabet; since the third letter of the keyword is `D`, the third letter should be moved three letters further on in the alphabet. So the output will be `DSUF`.

6. Find the unique $x \in \{0, 1, 2, \cdots, 493\}$ such that $x \equiv 3 \pmod{13}$ and $x \equiv 2 \pmod{38}$.

Solution Firstly find integer s and t such that $1 = s \cdot 13 + t \cdot 38$. One can find that $1 = 3 \cdot 13 - \cdot 38$. Then $x \equiv 2 \cdot 3 \cdot 13 - 3 \cdot 38 \equiv -36 \pmod{494}$ Finally, we need to add 494 to the answer to get 458.

7. Find which element of $\{1, 2, \cdots, 46\}$ is inverse to 38 modulo 47.

Solution The Euclidean Algorithm applied to 47 and 38 gives

$$47 = 38 + 9$$
$$38 = 4 \times 9 + 2$$
$$9 = 4 \times 2 + 1$$

Rearranging this information (or using the extended Euclidean algorithm), we get that $1 = 17 \times 47 - 21 \times 38$. So -21 is an inverse of 38 modulo 47, and the desired answer is 26.

8. Suppose that an RSA cryptosystem has a public key of $(46, 3)$. Encrypt the message $[2, 4]$.

Solution To encrypt, we raise each letter of the plaintext to the power 3 and reduce modulo 46. Since $4^3 = 64 \equiv 18 \pmod{46}$, the answer is $[8, 18]$.

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

```
> p:=NextPrime(1024);
> n:=p*p*p;
> EulerPhi(n) mod p;
```

Solution These commands tell MAGMA to let p be the next prime after 1000 (which is actually 1031, but we don't need to know that), then let $n = p^3$ and find the residue of $\varphi(n)$ modulo p. Since $\varphi(p^3) = p^2(p-1)$, the answer is 0.

10. Find the residue of 3^{6004} modulo 77.

Solution The prime factorization of 77 is 7×11, so $\varphi(77) = 6 \times 10 = 60$. Since $6004 \equiv 4 \pmod{60}$, we have $3^{6004} \equiv 3^4 = 81 \pmod{77}$, so the answer is $81 - 77 = 4$.

An alternative is to find the residue of 3^{6004} modulo the primes 7 and 11 separately, and then combine that information by solving a system of simultaneous congruences.

11. If a transposition cipher encrypts the word `MELON` as `ENOML`, what is the **decryption** of `RENCO`?

Solution A transposition cipher permutes the letters of the plaintext according to some fixed permutation. In this case we see that the first letter goes to fourth place, the second letter goes to first place, the third letter goes to fifth place, fourth letter to third place and fifth letter to second place. So the decryption of `RENCO` is `CRONE`.

12. Find $\sigma(2407)$, the sum of all the positive integer divisors of 2407.

Solution Since 2407 has prime factorization 29×83, its positive divisors are $1, 29, 83, 2407$. So the answer is 2520.

13. Find $\gcd(3^{100} - 1, 35)$.

Solution

Prime factors of 35 are 5 and 7. So we check the divisibility of $3^{100} - 1$ by each of those factors independently. $5 - 1$ definitely divides 100 therefore, by Fermat Little Theorem, $5 \mid 3^{100} - 1$. Also, $3^6 \equiv 1 \pmod{7}$ and therefore $3^{100} \equiv 3^4 \not\equiv 1 \pmod{7}$. Therefore the final answer is 5.

Alternatively, one can use the Euler-Fermat theorem straight away.

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

```
> n:=125;
> Factorial(n-1) mod (n^8);
```

Solution These commands tell MAGMA to find the residue of 124! modulo $125^8 = 5^{24}$. Since 24 of the terms in 124! are multiples of 5, 124! is divisible by 5^{24}. Therefore the answer is 0.

15. Function f is defined as follows:

$$f(n) := \sum_{d \mid n} \mu(d) \cdot d^2,$$

where $\mu(n)$ is the Möbius function. Compute $f(324)$.

Solution $\mu(d)$ and d^2 are both multiplicative. Therefore their product and in turn $f(n)$ is multiplicative too. The prime factorization of 324 is $2^2 \cdot 3^4$.

Hence we have

$$f(324) = f(4) \cdot f(81) = (1 - 2^2)(1 - 3^2) = 24.$$