Problem 1.32

1. For which of the following primes is 2 a primitive root modulo p?
2. p = 7

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 1; 2^4 = 2; 2^5 = 4;

Answer: NO

1. p = 13

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 3; 2^5 = 6; 2^6 = 12; 2^7 = 11; 2^8 = 9;

2^9 = 5; 2^10 = 10; 2^11 = 7;

Answer: YES

1. p = 19

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 =13; 2^6 = 7; 2^7 = 14; 2^8 = 9;

2^9 = 18; 2^10 = 17; 2^11 = 15; 2^12 = 11; 2^13 = 3; 2^14 = 6; 2^15 = 12;

2^16 = 5; 2^17 = 10;

Answer: YES

1. p = 23

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 = 9; 2^6 = 18; 2^7 = 13; 2^8 = 3;

2^9 = 6; 2^10 = 12; 2^11 = 1; 2^12 = 2; 2^13 = 4; 2^14 = 8; 2^15 = 16;

2^16 = 9; 2^17 = 18; 2^18 = 13; 2^19 = 3; 2^20 = 6; 2^21 = 12;

Answer: NO

1. For which of the following primes is 3 a primitive root modulo p?
2. p = 5

3^0 = 1; 3^1 = 3; 3^2 = 4; 3^3 = 2;

Answer: YES

1. p = 7

3^0 = 1; 3^1 = 3; 3^2 = 2; 3^3 = 6; 3^4 = 4; 3^5 = 5;

Answer: YES

1. p = 11

3^0 = 1; 3^1 = 3; 3^2 = 9; 3^3 = 5; 3^4 = 4; 3^5 = 1; 3^6 = 3; 3^7 = 9; 3^8 = 5;

Answer: NO

1. p = 17

3^0 = 1; 3^1 = 3; 3^2 = 9; 3^3 = 10; 3^4 = 13; 3^5 = 5; 3^6 = 15; 3^7 = 11;

3^8 = 16; 3^9 = 14; 3^10 = 8; 3^11 = 7; 3^12 = 4; 3^13 = 12; 3^14 = 2; 3^15 = 6;

Answer: YES

c) Find a primitive root for each of the following primes.

i) p = 23

Answer: 2 is a primitive root.

Explanation: 2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 = 9; 2^6 = 18;

2^7 = 13; 2^8 = 3; 2^9 = 6; 2^10 = 12; 2^11 = 1; 2^12 = 2; 2^13 = 4;

2^14 = 8; 2^15 = 16; 2^16 = 9; 2^17 = 18; 2^18 = 13; 2^19 = 3; 2^20 = 6;

2^21 = 12;

ii) p = 29

Answer: 2 is a primitive root.

Explanation: 2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 = 3; 2^6 = 6;

2^7 = 12; 2^8 = 24; 2^9 = 19; 2^10 = 9; 2^11 =18; 2^12 = 7; 2^13 = 14;

2^14 = 28; 2^15 = 27; 2^16 = 25; 2^17 = 21; 2^18 = 13; 2^19 = 26; 2^20 = 23;

2^21 = 17; 2^22 = 5; 2^23 = 10; 2^24 = 20; 2^25 = 11; 2^26 = 22; 2^27 = 15;

iii) p = 41

Answer: 6 is a primitive root

Explanation: 6^0 = 1; 6^1 = 6; 6^2 = 36; 6^3 = 11; 6^4 = 25; 6^5 = 27; 6^6 = 39;

6^7 = 29; 6^8 = 10; 6^9 = 19; 6^10 = 32; 6^11 = 28; 6^12 = 4; 6^13 = 24;

6^14 = 21; 6^15 = 3; 6^16 = 18; 6^17 = 26; 6^18 = 33; 6^19 = 34; 6^20 = 40;

6^21 = 35; 6^22 = 5; 6^23 = 30; 6^24 = 16; 6^25 = 14; 6^26 = 2; 6^27 = 12;

6^28 = 31; 6^29 = 22; 6^30 = 9; 6^31 = 13; 6^32 = 37; 6^33 = 17; 6^34 = 20;

6^35 = 38; 6^36 = 23; 6^37 = 15; 6^38 = 8; 6^39 = 7;

iv) p = 43

Answer: 3 is a primitive root

Explanation: 3^0 = 1; 3^1 = 3; 3^2 = 9; 3^3 = 27; 3^4 = 38; 3^5 = 28; 3^6 = 41;

3^7 = 37; 3^8 = 25; 3^9 = 32; 3^10 = 10; 3^11 = 30; 3^12 = 4; 3^13 = 12;

3^14 = 36; 3^15 = 22; 3^16 = 23; 3^17 = 26; 3^18 = 35; 3^19 = 19; 3^20 = 14;

3^21 = 42; 3^22 = 40; 3^23 = 34; 3^24 = 16; 3^25 = 5; 3^26 = 15; 3^27 = 2;

3^28 = 6; 3^29 = 18; 3^30 = 11; 3^31 = 33; 3^32 = 13; 3^33 = 39; 3^34 = 31;

3^35 = 7; 3^36 = 21; 3^37 = 20; 3^38 = 17; 3^39 = 8; 3^40 = 24; 3^41 = 29;

d) Find all primitive roots modulo 11. Verify that there are exactly φ(10) of them, as asserted in Remark 1.33.

Answer: 11 has 4 primitive roots. {2, 6, 7, 8}

φ(10) = 4 and there are 4 of them.

Explanation: p = 11

Primitive root: 2

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 5; 2^5 = 10; 2^6 = 9; 2^7 = 7; 2^8 = 3; 2^9 = 6;

Primitive root: 6

6^0 = 1; 6^1 = 6; 6^2 = 3; 6^3 = 7; 6^4 = 9; 6^5 = 10; 6^6 = 5; 6^7 = 8; 6^8 = 4; 6^9 = 2;

Primitive root: 7

7^0 = 1; 7^1 = 7; 7^2 = 5; 7^3 = 2; 7^4 = 3; 7^5 = 10; 7^6 = 4; 7^7 = 6; 7^8 = 9; 7^9 = 8;

Primitive root: 8

8^0 = 1; 8^1 = 8; 8^2 = 9; 8^3 = 6; 8^4 = 4; 8^5 = 10; 8^6 = 3; 8^7 = 2; 8^8 = 5; 8^9 = 7;