Do the following exercises from the text:
Section 7.1: 6

6. Filnd a positive integer n for which there exist at least three distinct representations of n as the sum of two nonzero squares (disregarding order and sign).

▶ **Solution.** Since $(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bd)^2$ and any prime congruent to 1 modulo 4 can be written as a sum of two squares, for an integer with at least 3 prime factors congruent to 1 modulo 4 so that they can be rearranged in 3 different factorizations. Take $n = 5 \cdot 13 \cdot 17 = 1105$. Then

$$\begin{aligned}1105 &= (2^2+1^2)(3^2+2^2)(4^2+1^2) = (8^2+1^2)(4^2+1^2) = (32+1)^2+(8-4)^2 = \boxed{33^3+4^2}\\ &= (1^2+8^2)(4^2+1^2) = (4+8)^2+(1-32)^2 = \boxed{12^2+31^2}\\ &= (2^2+1^2)((12+2)^2+(3-8)^2) = (2^2+1^2)(14^2+5^2)\\ &= (2^2+1^2)(5^2+14^2) = (10+14)^2+(28-5)^2 = \boxed{24^2+23^2}.\end{aligned}$$

◀

Section 5.7: 1, 2, 3, 4, 6, 20

1. By direct calculation determine the following.

(a) $\mathrm{ord}_{17} 2$

▶ **Solution.** Modulo 17, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16 \equiv -1$, $2^5 \equiv -2$, $2^6 \equiv -4$, $2^7 \equiv -8$, $2^8 \equiv -16 \equiv 1$. Thus, $\mathrm{ord}_{17} 2 = 8$. ◀

(b) The least residue of each of 2^{20}, 2^{1024}, 2^{500} modulo 17.

▶ **Solution.** Modulo 17, $2^{20} \equiv 2^{8\cdot 2+4} \equiv 1^2 2^4 \equiv 16$, $2^{1024} \equiv 2^{8\cdot 128} \equiv 1^{128} \equiv 1$, and $2^{500} \equiv 2^{8\cdot 62+4} \equiv 1^{62}2^4 \equiv 16$. ◀

2. For which positive exponents e is $2^e \equiv \pmod{17}$?

▶ **Solution.** From problem 1 (a) $\mathrm{ind}_{17} 2 = 8$. Thus, $2^e \equiv 1 \pmod{17}$ if and only if $8 \mid e$. That is, $e = 8k$ for some $k \geq 0$. ◀

3. Determine $\mathrm{ord}_{17} 2^{12}$

▶ **Solution.** $(2^{12})^2 = 2^{24} = 2^{8\cdot 3} = (2^8)^3 \equiv 1^3 \equiv 1 \pmod{17}$. Therefore, $\mathrm{ord}_{17} 2^{12} \mid 2$ so $\mathrm{ord}_{17} 2^{12} = 1$ or 2. Since $2^{12} = 2^{8+4} = 2^8 2^4 \equiv 1 \cdot 16 \equiv 16 \not\equiv 1 \pmod{17}$, it follows that $\mathrm{ord}_{17} 2^{12} = 1$. ◀

4. By direct calculation, show that 3 is a primitive root modulo 17 and construct a table of indices to the base 3 modulo 17.

▶ **Solution.** Modulo 17 we have the following: $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 10$, $3^4 \equiv 13$, $3^5 \equiv 5$, $3^6 \equiv 15$, $3^7 \equiv 11$, $3^8 \equiv 16 \equiv -1$, $3^9 \equiv -3 \equiv 14$, $3^{10} \equiv -9 \equiv 8$, $3^{11} \equiv -10 \equiv 7$, $3^{12} \equiv -13 \equiv 4$, $3^{13} \equiv 12$, $3^{14} \equiv 2$, $3^{15} \equiv 6$, $3^{16} \equiv 1$. Therefore, 3 has order 16 and is hence a primitive root modulo 17. The table of indices is then

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3 a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

◀

6. Use the table of indices of Exercise 4 to solve the following if possible.

(a) $7x \equiv 5 \pmod{17}$

▶ **Solution.** Applying ind_3 to the congruence gives $\operatorname{ind}_3(7x) \equiv \operatorname{ind}_3 5 \pmod{16}$. Thus $\operatorname{ind}_3 7 + \operatorname{ind}_3 x \equiv \operatorname{ind}_3 5 \pmod{16}$. From the index table, this gives $11 + \operatorname{ind}_3 x \equiv 5 \pmod{16}$ so that $\operatorname{ind}_3 x \equiv -6 \equiv 10 \pmod{16}$, which from the table gives $x \equiv 8 \pmod{17}$. ◀

(b) $x^7 \equiv 5 \pmod{17}$

▶ **Solution.** $\operatorname{ind}_3 x^4 \equiv \operatorname{ind}_3 5 \pmod{16}$ so $7 \operatorname{ind}_3 x \equiv 5 \pmod{16}$. Then $\operatorname{ind}_3 x \equiv 49 \operatorname{ind}_3 x \equiv 35 \equiv 3 \pmod{16}$. From the index table, $x \equiv 10 \pmod{17}$. ◀

(c) $x^8 \equiv 8 \pmod{17}$

▶ **Solution.** $\operatorname{ind}_3 x^8 \equiv \operatorname{ind}_3 8$ so $8 \operatorname{ind}_3 x \equiv 10 \pmod{16}$, but this linear congruence is not solvable since $(8, 16) = 8$ and $8 \nmid 10$. ◀

20. Find $\phi(28) = 12$ primitive roots modulo 29.

▶ **Solution.** Use the index table for the prime 29 on Page 244. According to the table, 2 is a primitive root modulo 29. According to a formula proved in class, $\operatorname{ord}_{29} 2^r = \frac{28}{(r, 28)}$ since the order of 2 modulo 29 is 28 when it is a primitive element. Thus, $\operatorname{ord}_{29} 2^r = 28$ if and only if $(r, 28) = 1$ and hence $a = 2^r$ is a primitive element modulo 29 if and only if $r = \operatorname{ind}_2 a$ is relatively prime to 28. The indices that are relatively prime to 28 are 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27. The a's with these indices are 2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15 and these are the primitive roots modulo 29. ◀

Additional Exercises.

1. Determine which of 2000, 2001, 2002, 2003, and 2004 can be written as a sum of two squares. For those that can, find a representation as a sum of two squares.

▶ **Solution.** $2000 = 2^4 \cdot 5^3 = 4^2 \cdot 5^2 \cdot 5 = 20^2 \cdot (2^2 + 1^2) = 40^2 + 20^2$

$2001 = 3 \cdot 23 \cdot 29$ so 2001 has a prime factor congruent to 3 modulo 4 (namely 3 and 23) appearing to an odd power. Hence 2001 cannot be written as a sum of two squares.

$2002 = 2 \cdot 7 \cdot 11 \cdot 13$ so 2002 has a prime factor congruent to 3 modulo 4 (namely 7 and 11) appearing to an odd power. Hence 2002 cannot be written as a sum of two squares.

$2003 \equiv 3 \pmod 4$ and hence cannot be written as a sum of two squares.

$2004 = 2^2 \cdot 3 \cdot 167$ so 2004 has a prime factor congruent to 3 modulo 4 (namely 3 and 167) appearing to an odd power. Hence 2004 cannot be written as a sum of two squares.

◀

2. Write the integers $3185 = 5 \cdot 7^2 \cdot 13$; $39690 = 2 \cdot 3^4 \cdot 5 \cdot 7^2$; and $62920 = 2^3 \cdot 5 \cdot 11^2 \cdot 13$ as a sum of two squares.

▶ **Solution.** $3185 = (2^2 + 1^2) \cdot 7^2 \cdot (3^2 + 2^2) = 7^2((6+2)^2 + ((4-3)^2) = 7^2(8^2 + 1^2) = 56^2 + 7^2$

$39690 = 2 \cdot 3^3 \cdot 5 \cdot 7^2 = 63^2 \cdot 10 = 63^2(3^2 + 1^2) = 189^2 + 63^2$.

$62920 = 2^3 \cdot 5 \cdot 11^2 \cdot 13 = 22^2 \cdot 2 \cdot 65 = 22^2(1^2 + 1^2)(8^2 + 1^2) = 22^2((8+1)^2 + (1-8)^2) = 22^2(9^2 + 7^2) = 198^2 + 154^2$. ◀

3. Is it true that if m and n are sums of two squares and $m \mid n$, then $\frac{n}{m}$ is a sum of two squares? Prove it is true or give a counterexample.

▶ **Solution.** This is true. To prove it, suppose that p is a prime congruent to 3 modulo 4 that divides $\frac{n}{m}$. Then $p \mid n$ and the exponent k of p in the prime factorization of n must be even. Let l be the exponent of p in the prime factorization of m. Then $0 \leq l \leq k$. Since, m is a sum of two squares, then l must be even. Thus the exponent of p in the prime factorization of $\frac{n}{m}$ is $k - l$, which is even. Since p is an arbitrary prime congruent to 3 modulo 4 and dividing $\frac{n}{m}$, it follows from Theorem 7.1 that $\frac{n}{m}$ can be written as a sum of two squares. ◀