

## Selected Solutions

**Page 108, #1:** Show that if  $p$  and  $q$  are different odd primes, and if  $(a, pq) = 1$ , then

$$a^{\phi(pq)/2} \equiv 1 \pmod{pq}.$$

**Proof:** Notice that

$$a^{\phi(pq)/2} = \left(a^{\phi(q)/2}\right)^{\phi(p)} \equiv 1 \pmod{p}$$

and

$$a^{\phi(pq)/2} = \left(a^{\phi(p)/2}\right)^{\phi(q)} \equiv 1 \pmod{q}.$$

Also notice that  $x = 1$  is a solution to

$$x \equiv 1 \pmod{p}$$

$$x \equiv 1 \pmod{q}$$

and to

$$x \equiv 1 \pmod{pq}.$$

Since  $a^{\phi(pq)/2}$  satisfies the first two equations, then by the uniqueness provided by the Chinese Remainder Theorem, we must also have

$$a^{\phi(pq)/2} \equiv 1 \pmod{pq}.$$

**Web Problem #1:** Find all the different solutions to the quadratic congruence

$$x^2 + 26x + 33 \equiv 0 \pmod{60}.$$

**Start of Proof:** We reduce this modulo 3, 4, and 5 and use the Chinese Remainder Theorem.

$$x^2 + x \equiv 0 \pmod{3}$$

$$x^2 + 2x + 1 \equiv 0 \pmod{4}$$

$$x^2 + x + 3 \equiv 0 \pmod{5}$$

These equations have the following solutions:

$$x \equiv 0, 1 \pmod{3}$$

$$x \equiv 1, 3 \pmod{4}$$

$$x \equiv 1, 3 \pmod{5}$$

Each combination of values chosen in this system corresponds to a unique solution modulo 60. From this point, you should know how to compute all 8 solutions.

**Web Problem #2b:** Deduce that

$$F_\phi(n) = \sum_{d|n} \phi(d) = n.$$

**Proof:** We know that  $F_\phi$  is a multiplicative function by Theorem 2.15. So we only need to compute  $F_\phi$  on powers of primes.

$$\begin{aligned} F_\phi(p^a) &= \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^a) \\ &= 1 + (p-1) + (p^2-p) + \cdots + (p^a - p^{a-1}) \\ &= 1 + (-1+p) + (-p+p^2) + \cdots + (-p^{a-1} + p^a) \\ &= p^a \end{aligned}$$

Therefore,

$$F_\phi(n) = F_\phi(p_1^{a_1}) \cdots F_\phi(p_k^{a_k}) = p_1^{a_1} \cdots p_k^{a_k} = n.$$

**Web Problem #4:** Let  $p \geq 7$  be a prime number. Show that one of 2, 5, and 10 is a quadratic residue modulo  $p$ . Deduce from this that there are two consecutive integers which are quadratic residues modulo  $p$ .

**Proof:** If either 2 or 5 is a quadratic residue modulo  $p$ , then the first statement is true. Suppose that neither 2 nor 5 is a quadratic residue modulo  $p$ . Then

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{5}{p}\right) = (-1) \cdot (-1) = 1,$$

so that 10 is a quadratic residue modulo  $p$ .

Notice that 1, 4, and 9 are always quadratic residues modulo  $p$ . Therefore, since at least one of 2, 5, and 10 is a quadratic residue modulo  $p$  (and 2, 5, and 10 are relative prime to  $p$  since  $p \geq 7$ ), there are always two consecutive integers which are quadratic residues modulo  $p$ .

**Web Problem #5:** Find all odd primes  $p$  such that -2 is a quadratic residue modulo  $p$ .

**Proof:** Notice that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right).$$

For -2 to be a quadratic residue modulo  $p$ , we must have both of these terms be +1 or both of these terms be -1.

For the +1 case, we must have  $p \equiv 1 \pmod{4}$  from the first term and  $p \equiv 1, 7 \pmod{8}$  from the second term. This can only happen when  $p \equiv 1 \pmod{8}$ .

For the -1 case, we must have  $p \equiv 3 \pmod{4}$  from the first term and  $p \equiv 3, 5 \pmod{8}$  from the second term. This can only happen when  $p \equiv 3 \pmod{8}$ .

Therefore, -2 is a quadratic residue modulo  $p$  when  $p \equiv 1, 3 \pmod{8}$ .

**Web Problem #6:** Show that there are infinitely many primes of the form  $8k + 3$ .

**Proof:** Suppose there are only finitely many such primes,  $p_1, \dots, p_r$ . Let  $Q = (p_1 \cdots p_r) + 2$ . Notice that the product of the  $p_i$  will either be 1 or 3 modulo 8, so that the product squared will be 1 modulo 8. Therefore,  $Q \equiv 3 \pmod{8}$ .

If  $Q$  is a prime, then we have a contradiction since  $Q$  is not one of the  $p_i$ . Therefore,  $Q$  is a composite and has a factorization into primes. None of the primes can be 3 modulo 8, so they must be 1, 5, and 7 modulo 8. Notice that products of numbers 1 and 5 modulo 8 can only be 1 or 5 modulo 8. Therefore, there must be some prime  $P$  which is 7 modulo 8.

From problem #5, we know that -2 is a quadratic residue modulo  $Q$ . But then -2 is a quadratic residue modulo  $p$  for any prime  $p$  dividing  $Q$ . In particular, -2 is a quadratic residue modulo  $P$ . But  $P$  is neither 1 nor 3 modulo 8, and so -2 cannot be a quadratic residue modulo  $P$ . This gives a contradiction, so there cannot be only finitely many primes of the form  $8k + 3$ .