Sheet 6

Due 17.30 Wednesday 28th February

Hand in solutions to questions 1b, 1c, 2b, 3b, 3c.

Please write your student ID number on your work and staple it together.

1. For each of the linear congruences below, decide whether it has solutions and if it does, find them all.

   (a) $10x \equiv 14 \mod 23$.

   Solution. Let $n = 23$. Then 10 is coprime to n, so we can invert 10 modulo n. The Euclidean Algorithm spits out $1 = 7 \times 10 - 3 \times 23$. So we have $7 \times 10 \equiv 1 \mod 23$ and hence $[10]^{-1} = [7]$. Therefore

   $$[10][x] = [14] \iff [7][10][x] = [7][14] \iff [x] = [7][14].$$

   We conclude $x \equiv 7 \times 14 \equiv 98 \equiv 6 \mod 23$.

   **(b) $10x \equiv 14 \mod 17$. (2 marks)

   Solution. Let $n = 17$. Then 10 is coprime to n, so we can invert 10 modulo n. The Euclidean Algorithm gives

   $$\begin{aligned} 17 &= 10 + 7, \\ 10 &= 7 + 3, \\ 7 &= 2 \times 3 + 1; \end{aligned}$$

   and

   $$\begin{aligned} 1 &= 7 - 2 \times 3 && && (1) \\ &= 7 - 2 \times (10 - 7) && = 3 \times 7 - 2 \times 10 && (2) \\ &= 3 \times (17 - 10) - 2 \times 10 && = 3 \times 17 - 5 \times 10. && (3) \end{aligned}$$

   So we have $(-5) \times 10 \equiv 1 \mod 17$ and hence $[10]^{-1} = [-5]$. Therefore

   $$[10][x] = [14] \iff [-5][10][x] = [-5][14] \iff [x] = [-5][14].$$

   We conclude $x \equiv -5 \times 14 \equiv 15 \mod 17$.

   Notice that we have set $n = 17$, so [10] means the class of residues of congruent to 10 modulo 17. In part (a) we set $n = 23$, so [10] meant the class of residues congruent to 10 modulo 23.

   **(c) $10x \equiv 14 \mod 21$. (2 marks)

   Solution. Let $n = 21$. Then 10 is coprime to n, so we can invert 10 modulo n. We have

   $$21 = 2 \times 10 + 1;$$

and so

$$1 = 21 - 2 \times 10 \tag{4}$$

and $(-2) \times 10 \equiv 1 \mod 21$. Hence $[10]^{-1} = [-2]$. Therefore

$$[10][x] = [14] \iff [-2][10][x] = [-2][14] \iff [x] = [-2][14].$$

We conclude $x \equiv -2 \times 14 \equiv 14 \mod 21$.

2. (a) Show that 71 is prime.

   Solution. Detailed version: Suppose for a contradiction that 71 is composite (not prime). Then $71 = nm$ where n and m are numbers other than 1 and 71. At least one of n and m must be less than or equal to $\sqrt{71}$, because if $n > \sqrt{71}$ then $m = 71/n < \sqrt{71}$. Let's say that $n \le \sqrt{71}$. Then n has a prime divisor p with $p \le \sqrt{71}$. Then p divides 71. So we just need to show that 71 has no prime divisors p with $p \le \sqrt{71}$. Since $\sqrt{71} < \sqrt{81} = 9$ we only need to check primes less than 9. We see that 2, 3, 5 and 7 do not divide 71. So 71 is prime.

   Short version (also valid): $p \le \sqrt{71}$. Then 71 has a prime divisor p with $p \le \sqrt{71}$. Since $\sqrt{71} < \sqrt{81} = 9$ this means $p = 2$, 3, 5 or 7. None of these divides 71. So 71 is prime.

   **(b) Find $\phi(71)$ and calculate 5^{209} modulo 71 and 12^{142} modulo 71. (2 marks)

   Solution. The number 71 is prime, so $\phi(71) = 70$. Let $n = 71$. Then

$$[5]^{209} = [5]^{3\times 70-1} \qquad = [5]^{-1}.$$

   We invert 5 modulo 71. We have $71 = 14 \times 5 + 1$ so $(-14) \times 5 \equiv 1 \mod 71$. Therefore $[5]^{209} = [5]^{-1} = [-14]$. So $5^{209} \equiv -14 \equiv 57 \mod 71$.

   Similarly

$$\begin{aligned}[12^{142}] = [12]^{2\times 70+2} &\qquad = [12]^2 \\ = [12^2] &\qquad = [144]\end{aligned}$$

   so $12^{142} \equiv 144 \equiv 2 \mod 71$.

3. In the context of public key cryptography, let p and q be primes. Let the pair (pq, a) be the public key in the RSA algorithm for encryption, and let (pq, c) be the private key.

   Let r be any integer with $(r, pq) = 1$.

   (a) Show that a and c are odd.

Solution. We have $ac \equiv 1 \mod \phi(pq)$. So ac is coprime to $\phi(pq)$. Since p and q are prime we have $\phi(pq) = (p-1)(q-1)$. All primes except for 2 are odd. So one of p and q must be odd, and one of $p-1$ and $q-1$ must be even. So $\phi(pq)$ is even. Since ac is coprime to $\phi(pq)$, we must have ac odd, because otherwise 2 would divide both ac and $\phi(pq)$. Since ac is odd, a and c are odd.

All three parts of this question are about properties of the public and private key. The most important property is that $ac \equiv 1 \mod \phi(pq)$. The third part of the question gives us a way to find p and q given the public and private keys, by finding $\gcd(k+1, pq)$ and $\gcd(k-1, pq)$.

**(b) Given that a and c are odd, let $k \equiv r^{\frac{ac-1}{2}} \mod pq$. Show that $k^2 \equiv 1 \mod pq$. (2 marks)

Solution. We have

$$k^2 \equiv r^{ac-1} \mod pq.$$

We also have $ac \equiv 1 \mod \phi(pq)$. So $\phi(pq)$ divides $ac-1$. So by Theorem 2.15 from the lecture notes, we have $r^{ac-1} \equiv 1 \mod pq$. So $k^2 \equiv 1 \mod pq$.

**(c) Given that $k^2 \equiv 1 \mod pq$, show that $(k+1)(k-1) \equiv 0 \mod p$. Deduce that either p divides $(k+1)$ or p divides $(k-1)$. (2 marks)

Solution. We have

$$(k+1)(k-1) = k^2 - 1 \equiv 0 \mod pq$$

since $k^2 \equiv 1 \mod pq$. So pq divides $(k+1)(k-1)$. In particular p divides $(k+1)(k-1)$. By Theorem 2.8 from the lecture notes, either p divides $(k+1)$ or p divides $(k-1)$.

4. Let $\phi(n)$ be Euler's totient function. Prove that if m is odd, then $\phi(2m) = \phi(m)$.

   Solution. Since $(2, m) = 1$, and the function ϕ is multiplicative, we have $\phi(2m) = \phi(m)\phi(2)$. As $\phi(2) = 1$, the claimed result follows.