DISCRETE MATH 37181 HOMEWORK SHEET 8

Instructions. Try these sometime after your tutorial and before the next lecture. Set aside some time each week to keep up with the homework. Partial solutions at the end of the PDF.

1. (a) Write 341 as $\sum b_i 2^i$ for $b_i \in \{0, 1\}$. [1]

   (b) Using repeated squaring, or otherwise, the remainder of 2^{85} on division by 31 is

   A. 1 C. 3 E. 0

   B. 2 D. 4 F. none of (A)–(E).

2. Prove or disprove:

   Let $q \in \mathbb{Z}$. If q is not divisible by 3, then $q^2 \equiv 1 \mod 3$.

3. (a) Using the Euclidean algorithm, or otherwise, $\gcd(1480, 139) =$

   A. 3 C. 9 D. 7

   B. 1 D. 13 E. none of (A)–(E).

   (b) Using the Euclidean algorithm backwards, or otherwise, find $d \in \mathbb{Z}_{1480}$ so that

   $$139 \cdot d \equiv 1 \mod 1480$$

   (this d is called the *multiplicative inverse* of 139 in $\mathbb{Z}_{1480}$). [2]

5. Let ϕ denote Euler's phi function. $\phi(49) =$

   A. 7 C. 41 E. none of (A)–(D).

   B. 42 D. 8

6. Use the formula from the lecture [3] to add the missing check digit for this ISBN

   $$978 - 0 - 19 - 852254 - x$$

Date: Week 8.

[1] i.e. write 341 in binary, or as its 2-ary expansion. For example, $35 = 32 + 2 + 1 = 1.2^5 + 0.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 1.2^0$ so in binary $32 = 100011_2$

[2] Recall: $\mathbb{Z}_{1480} = \{0, 1, 2, \ldots, 1479\}$, the set of remainders mod 1480.

[3] $\sum_{j=0}^{6} a_{2j+1} + \sum_{j=1}^{6} 3a_{2j} \equiv 0 \mod 10$

Brief solutions:

1. (a) $341 = 256 + 64 + 16 + 4 + 1$

   (b) A. 1.

   $85 = 64 + 16 + 4 + 1.$

   $2^2 = 4$
   $2^4 = 2^2.2^2 = 4.4 = 16$
   $2^8 = 2^4.2^4 = 16.16 = 256 \equiv 8 \mod 31$
   $2^{16} = 2^8.2^8 \equiv 8.8 = 64 \equiv 2 \mod 31$
   $2^{32} \equiv 4$
   $2^{64} \equiv 16$

   so $2^{85} = 2^{64}.2^{16}.2^4.2^1 \equiv 16.2.16.2 = 16^2.2^2 \equiv 8.4 = 32 \equiv 1 \mod 31.$

2. *Proof.* If q is not divisible by 3 then $\exists n \in \mathbb{Z}$ and $i \in \{1, 2\}$ such that $q = 3n + i$.

   Then $q^2 = 9n^2 + 6ni + i^2 = 3(3n^2 + 2ni) + i^2 \equiv i^2 \mod 3.$

   If $i = 1$ then $i^2 = 1$, and if $i = 2$ then $i^2 = 4 \equiv 1 \mod 3$ so the result follows by transitivity of the relation $\equiv \mod 3$. □

3. B. 1.

   (Notice $139 = 13^2$ and 13 does not divide 1480, or do the algorithm:)

   $1480 = 10.139 + 90$
   $139 = 1.90 + 49$
   $90 = 1.49 + 41$
   $49 = 1.41 + 8$
   $41 = 5.8 + 1$

4. $1 = 41 - 5.8$
   $= 41 - 5(49 - 41) = 6.41 - 5.49$
   $= 6.(90 - 49) - 5.49 = 6.90 - 11.49$
   $= 6.90 - 11.(139 - 90) = 17.90 - 11.139$
   $= 17.(1480 - 10.139) - 11.139 = 17.1480 - 181.139$

   so $d = -181 \equiv 1299 \mod 1480$. We usually give the d as a number between 0 and 1480.

5. 42.

6. We need $9 + 21 + 8 + 0 + 1 + 27 + 8 + 15 + 2 + 6 + 5 + 12 + x$
   $\equiv 9 + 1 + 8 + 0 + 1 + 7 + 8 + 5 + 2 + 6 + 5 + 2 + x$
   $\equiv 4 + x$ so we need $x = 6$.