Université Gustave Eiffel
M2 – Semester 1 – 2025/2026

Programming

CHAU Dang Minh

Exercise. **(Divisibility Problem)** We try to derive a divisibility rule for each integer m. That is, we find small a, b such that for each integer $n = 10d + u$,

$$m \mid 10d + u \iff m \mid ad + bu.$$

1. Try to generate such rule for each integer m.
2. Look at the results for inputs up to 200. Give explanations.

Solution. We will find integers a, b such that $0 \leq a \leq 10$ and $1 - m \leq b \leq m - 1$. Since d is much larger than u most of the cases, it is reasonable use the following order: $(a_1, b_1) < (a_2, b_2)$ if $a_1 < a_2$ or ($a_1 = a_2$ and $b_1 < b_2$). The solution will be the smallest pair (a, b) satisfying the condition. The equivalence

$$m \mid a_1 d + b_1 u \iff m \mid a_2 d + b_2 u$$

is maintained during the following transformations:

1. $a_2 = a_1 + \ell m$ or $b_2 = b_1 + \ell m$ for some integer ℓ.
2. $a_2 = \ell a_1$ and $b_2 = \ell b_1$ for some integer ℓ coprime with m.
3. $a_1 = \ell a_2$ and $b_1 = \ell b_2$ for some integer ℓ coprime with m.

Define a sequence of transformations

$$(a_0, b_0) = (10, 1), (a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k) = (a, b).$$

Let $c = \gcd(m, 10) \in \{1, 2, 5, 10\}$. We see that c divides a_i for each $i \in [0, k]$. We will prove that the minimal $a = c$ can be achieved i.e. there exists a sequence of transformations such that $a = c$.

Lemma 1. *There exists an integer x such that $10x \equiv c$ mod m and $\gcd(x, m) = 1$.*

Proof. Let $m = \prod_{\alpha \in I} p_\alpha^{e_\alpha}$ be the prime factorization of m. For each $\alpha \in I$, we have $10x \equiv c \bmod p_\alpha^{e_\alpha}$. Consider the following cases.

1. If $p_\alpha = 2$, then

$$10x \equiv c \bmod p_\alpha^{e_\alpha} \iff 5x \equiv \frac{c}{2} \bmod 2^{e_\alpha - 1} \iff 5x \equiv \frac{c}{2} \bmod 2^{e_\alpha - 1},$$

where the second equivalence is valid since p_α and 5 are coprime. We also have $c \in \{2, 10\}$, so $\frac{c}{2} \in \{1, 5\}$ and thus x is not divisible by 2.

2. If $p_\alpha = 5$, then

$$10x \equiv c \bmod p_\alpha^{e_\alpha} \iff 2x \equiv \frac{c}{5} \bmod 5^{e_\alpha - 1} \iff x \equiv \frac{c}{5} \cdot 2^{-1} \bmod 5^{e_\alpha - 1}.$$

Again, the second equivalence is valid since p_α and 5 are coprime. We also have $c \in \{5, 10\}$, so $\frac{c}{5} \in \{1, 2\}$ and thus x is not divisible by 5.

3. Otherwise, p_α is coprime with 10. We have

$$10x \equiv c \bmod p_\alpha^{e_\alpha} \iff x \equiv 10^{-1}c \bmod p_\alpha^{e_\alpha}.$$

   We also have $c \in \{1, 2, 5, 10\}$, which is all coprime with p_α. Thus, x is not divisible by p_α.

By the Chinese Remainder Theorem, there exists an integer x satisfying one of the congruences for $(\alpha_i)_{i\in I}$. We have $\gcd(x, m) = 1$ since for each prime factor p_α of m, x is not divisible by p_α. □

By the lemma, there exists an integer x such that $10x \equiv c \bmod m$ and $\gcd(x, m) = 1$. We have the following sequence of transformations:

$$(10, 1) \longrightarrow (10x, x) \longrightarrow (c, x) \longrightarrow (c, x \bmod m) \longrightarrow (c, x \bmod m - m).$$

Now we will construct such an x. A straightforward way is to find x_{p_i} satisfying $10x_{p_i} \equiv c \bmod p_i^{ei}$ for each prime factor p_i of m, then use the Chinese Remainder Theorem to find x. However, it is not efficient since the factorization of m is required. It is surprising that using the Extended Euclidean algorithm (EEA) is sufficient. We learn from the proof of Lemma 1 to prove our following results.

Lemma 2. *Let x_0, y_0 be integers such that $10x_0 + my_0 = c$. Let $s = \frac{m}{c}$. Then the set*

$$\{x_0, x_0 + s, x_0 + 2s, x_0 + 3s\}$$

contain an integer x such that $\gcd(x, m) = 1$.

Proof. Let $n = 2^\alpha 5^\beta r$. Then

$$c = \gcd(m, 10) = 2^{\min(\alpha,1)}5^{\min(\beta,1)} \text{ and } s = 2^{\alpha-\min(\alpha,1)}5^{\beta-\min(\beta,1)}r.$$

Consider a prime factor p of m.

1. If $p = 2$ i.e. $\alpha \geq 1$. We have two cases.
   - $\alpha = 1$. Then $s = 5^{\beta-\min(\beta,1)}r$ is odd. Thus, there are exactly two odd numbers and two even numbers in the set $\{x_0, x_0 + s, x_0 + 2s, x_0 + 3s\}$.
   - $\alpha \geq 2$. Then $5x_0 \equiv c \bmod 2^{\alpha-1}$ and x_0 is odd. Also, $s = 2^{\alpha-1}5^{\beta-\min(\beta,1)}r$ is even. Thus, all numbers in the set $\{x_0, x_0 + s, x_0 + 2s, x_0 + 3s\}$ are odd.
2. If $p = 5$ i.e. $\beta \geq 1$. We have two cases.
   - $\beta = 1$. Then $s = 2^{\alpha-\min(\alpha,1)}r$ is not divisible by 5. Checking all possible cases of x_0 and s in modulo 5, there are at least *three* numbers that are not divisible by 5.
   - $\beta \geq 2$. Then $2x_0 \equiv \frac{c}{5} \bmod 5^{\beta-1}$ and x_0 is not divisible by 5. Also, $s = 2^{\alpha-\min(\alpha,1)}5^{\beta-1}r$ is divisible by 5. Thus, all numbers in the set $\{x_0, x_0 + s, x_0 + 2s, x_0 + 3s\}$ are not divisible by 5.
3. Otherwise, p is coprime with 10. We have $x_0 \equiv 10^{-1}c \bmod p^e$. Since $c \in \{1, 2, 5, 10\}$, s is divisible by p. Thus, all numbers in the set $\{x_0, x_0 + s, x_0 + 2s, x_0 + 3s\}$ are not divisible by p.

Therefore, we have to consider four cases for α and β. Each guarantees at least one number in the set $\{x_0, x_0 + s, x_0 + 2s, x_0 + 3s\}$ is not divisible by either 2 or 5. In fact, only in the case that $\alpha = \beta = 1$ do we have to use the pigeonhole principle. □

From the proof of Lemma 2, an integer x in the set satisfies if x is not divisible by 2 or 5. Moreover, the only edge case is when $\alpha = \beta = 1$ i.e. $m = 10r$ where r is coprime with 10. But in such cases, EEA returns $x_0 = 1$, which is automatically coprime with m. Therefore, we have a stronger result although there is almost no difference in practice.

Lemma 3. *Let x_0, y_0 be integers such that $10x_0 + my_0 = c$ and x_0 is returned by EEA. Let $s = \dfrac{m}{c}$. Then the set*

$$\{x_0, x_0 + s, x_0 + 2s\}$$

contain an integer x such that $\gcd(x, m) = 1$.

Thus, the algorithm to find a divisibility rule for m is as follows.

```
$(x_0, y_0, c) \leftarrow \mathrm{EEA}(m, 10)$, $s \leftarrow m/c$.
if $2 \mid x_0$ then
    return $(c, (x_0 + s) \bmod m - m)$.
else
    if $5 \nmid x_0$ then
        return $(c, x_0 \bmod m - m)$.
    else
        return $(c, (x_0 + 2s) \bmod m - m)$.
```

Proposition 1. *The above algorithm returns the optimal divisibility rule for each integer m in $O(1)$.*

Proof. The correctness of the algorithm is guaranteed by the previous lemmas. The time complexity is $O(\log(\min(m, 10))) = O(1)$ since 10 is a constant. □