$z \in \mathbb{Z}$

$xm + yn = z,$

$0 \le x \le n-1$

$7x + 11y = 59$

$7x \equiv 4 \pmod{11}$

$4y \equiv 3 \pmod 7$

$y \equiv 6 \pmod 7$

$4^{-1} \equiv 2 \pmod 7$

$y = 1 \quad 53 - 11 = 42$

$x = 6$

$(n-1)m + yn = mn - m + yn > mn - m - n$

$xm + yn = mn - m - n$

$xm \equiv -m \pmod n \qquad x, y \ge 0$

$x \equiv -1 \equiv n-1 \pmod n$

$yn \equiv -n \pmod m$

$y = -1$

$6 \equiv -1 \pmod 7$

$\gcd(m,n) = 1 \qquad mn - m + yn = mn - n - m$

$xm + yn = z \qquad \Rightarrow yn = -n$

$\Rightarrow y = -1 < 0$ Contradict

$x \equiv z m^{-1} \pmod n$

$y \equiv z n^{-1} \pmod m$

$z = 100$

$n = 7$

$x \equiv m^{-1} \pmod n$

$mx \equiv 1 \pmod n$

$m^{-1} \cdot z = 100 m^{-1}$

$\equiv 2m^{-1}$

$\equiv 12 \equiv 5 \pmod 7$

$mx + ny = 1$

$53 - 52 = 1$

$mn - n + n$

$1 \cdot 53 + (-4) 13 = 1 \leftarrow mn - m - n$

$x \quad y$

$y = -1$

$y = -2$

$y = 1$

$n - 1 \pmod n$

$2n - 1$

$3n - 1$

$0 \le x \le n-1$

$n-1$

$xm + yn = z > mn - m - n \qquad xm + yn = mn - m - n$

$\le nm - m + yn$

RHS

$y < 0$

$\ge 0$

$mn - m - n \le mn - m - n$

$mn - m - 2n \le mn - m - n$

$n-1$

$xm + yn$

$(n-1)m + yn$

$= \cancel{mn} - \cancel{m} + yn > \cancel{mn} - \cancel{m} - n$

$\Rightarrow yn > -n$

$\Rightarrow y > -1 \qquad \Rightarrow y \ge 0$

$J_1, J_2, \ldots, J_n \qquad J_1 > J_2 \qquad n^2 \qquad n^2 - 1 = (n+1)(n-1) \ge n(n-1)$

rejections — job — rej

$(n-1)^2 + 1$

$C_1 \; \cancel{J_2} \; J_1$

$C_2 \; \cancel{J_1} \; J''$

$\vdots$

$n-1$

$n \qquad C_n \; \cancel{J_1} \; J'$

$C_1 \quad J_1$

$n-1 \left\{ C_2, C_3, \ldots, C_n \right.$

$n-2$

$(n-1)$ jobs $(J_2, J_3, \ldots, J_n)$

$(n-2)$ rej

$+$

$(n-1)$ rej

$= (n-1)^2$ rej

$(n-1)^2 + 1$ days

| | | | |
|---|---|---|---|
| $C_1$ | $\ast$ 2 | 2 | $\cancel{3}$ 3 |
| $C_2$ | 3 | $\cancel{x}$ 1 | 1 |
| $C_3$ | | | 2 |

$z_i \pmod{n_j} \equiv \begin{cases} 1 & i = j \\ 0 & i \ne j \end{cases}$

$z_i = \left(\prod_{j \ne i} n_j\right)\left(\left(\prod_{j \ne i} n_j\right)^{-1} \pmod{n_i}\right)$

$z_i \pmod{n_j} \qquad j = i$

$z_3 = n_1 n_2 \left((n_1 n_2)^{-1} \pmod{n_3}\right)$

$x \equiv a_1 z_1 + a_2 z_2 + a_3 z_3 \pmod{\prod_i n_i}$

$x \equiv a_i \pmod{n_i}$

$a_i \cdot z_i \equiv a_i \pmod{n_i}$

$\sum a_i z_i$

$x \equiv 13 \pmod{30}$

$x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 3$

$x \equiv 3 \pmod 5$

~~[illegible]~~

$a_1 = 1$

$a_2 = 1$

$a_3 = 3$

$a_4 = 5$

$z_1 = 15(15^{-1} \pmod 2) = 15$

$z_2 = 10(10^{-1} \pmod 3) = 10$

$z_3 = n_1 n_2 ((n_1 n_2)^{-1} \pmod{n_3}) = 6$

$2, 6, 10, 14, \ldots$

$2 \quad 1 \quad 0 \quad 4$

$z_3 \pmod{n_i} \equiv \begin{cases} 1 & \text{if } i = 3 \\ 0 & \text{o/w} \end{cases}$

$6 \equiv 1 \pmod 5$

$\equiv 2 \pmod 4$

$1 \cdot 15 + 1 \cdot 10 + 3 \cdot 6 \pmod{30}$

$\equiv 43 \equiv 13 \pmod{30}$

$14 \equiv 19^{-1} \pmod{53}$

114
106

$\rightarrow (3)19 + (-1)53 = 4$

$(6)19 + (-2)53 = 8$

$(-5)19 + (2)53 = 11$

$\rightarrow (-11)19 + (4)53 = 3$

$(14)19 + (-5)53 = 1$

$y \equiv b_i \pmod{n_i}$

$xy \equiv a_i b_i \pmod{n_i}$

# 1 Counting Cartesian Products

For two sets $A$ and $B$, define the cartesian product as $A \times B = \{(a,b) : a \in A, b \in B\}$.

(a) Given two countable sets $A$ and $B$, prove that $A \times B$ is countable.

(b) Given a finite number of countable sets $A_1, A_2, \ldots, A_n$, prove that

$$A_1 \times A_2 \times \cdots \times A_n$$

is countable.

# 2 Counting Functions

Are the following sets countable or uncountable? Prove your claims.

(a) The set of all functions $f$ from $\mathbb{N}$ to $\mathbb{N}$ such that $f$ is non-decreasing. That is, $f(x) \leq f(y)$ whenever $x \leq y$.

(b) The set of all functions $f$ from $\mathbb{N}$ to $\mathbb{N}$ such that $f$ is non-increasing. That is, $f(x) \geq f(y)$ whenever $x \leq y$.

# 3 Undecided?

Let us think of a computer as a machine which can be in any of $n$ states $\{s_1, \ldots, s_n\}$. The state of a 10 bit computer might for instance be specified by a bit string of length 10, making for a total of $2^{10}$ states that this computer could be in at any given point in time. An algorithm $\mathscr{A}$ then is a list of $k$ instructions $(i_0, i_2, \ldots, i_{k-1})$, where each $i_l$ is a function of a state $c$ that returns another state $u$ and a number $j$. Executing $\mathscr{A}(x)$ means computing

$$(c_1, j_1) = i_0(x), \qquad (c_2, j_2) = i_{j_1}(c_1), \qquad (c_3, j_3) = i_{j_2}(c_2), \qquad \ldots$$

until $j_\ell \geq k$ for some $\ell$, at which point the algorithm halts and returns $c_{\ell-1}$.

(a) How many iterations can an algorithm of $k$ instructions perform on an $n$-state machine (at most) without repeating any computation?

(b) Show that if the algorithm is still running after $2n^2k^2$ iterations, it will loop forever.

(c) Give an algorithm that decides whether an algorithm $\mathscr{A}$ halts on input $x$ or not. Does your contruction contradict the undecidability of the halting problem?

# 4 Code Reachability

Consider triplets $(M,x,L)$ where

```
M is a Java program
x is some input
L is an integer
```

and the question of: if we execute $M(x)$, do we ever hit line $L$?

Prove this problem is undecidable.