Homework 3, due Tuesday Jan 27 at 1pm

1. Assume p is a prime and $r = r_0 + r_1 p + \ldots + r_n p^n$ has an expansion in base p with digits r_i. Recall our convention that $\binom{i}{j} = 0$ if $j > i$.

   Throughout, let p be prime.

   (a) (5 pts) Show that if $0 < k < p^m$, then $\binom{p^m}{k} \bmod p = 0$. Conclude that
   $$(1+x)^{p^m} \equiv 1 + x^{p^m} \pmod{p}.$$

   (b) (5 pts) Justify each congruence in the following:
   $$\begin{aligned}
   \sum_{s=0}^{r} \binom{r}{s} x^s &\equiv (1+x)^r \pmod{p} \\
   &\equiv \prod_{m=0}^{n} (1+x)^{r_m p^m} \pmod{p} \\
   &\equiv \prod_{m=0}^{n} (1+x^{p^m})^{r_m} \pmod{p} \\
   &\equiv \prod_{m=0}^{n} \sum_{s_m=0}^{r_m} \binom{r_m}{s_m} x^{s_m p^m} \pmod{p} \\
   &\equiv \sum_{s=0}^{r} \prod_{\substack{\{s_0,\ldots,s_k: \\ s = s_0 p^0 + \ldots + s^k p^k\}}} \binom{r_m}{s_m} x^s \pmod{p}
   \end{aligned}$$

   (c) (5 pts) Conclude Lucas's theorem. If the s_i are the base p digits of a number $s = s_0 + s_1 p + \ldots + s_n p^n$, then
   $$\binom{r}{s} \equiv \binom{r_n}{s_n} \cdots \binom{r_1}{s_1} \binom{r_0}{s_0} \pmod{p}$$

2. (40 pts) Prove the Davis-Putnam-Robinson theorem: if exponentiation is diophantine, then every r.e. set $R \subseteq \mathbb{N}$ is diophantine. Recall that in class, we used Lucas's theorem to prove that the bit masking relation $\preceq$ is diophantine.

   Recall the outline of our proof. We are given a register machine with r many registers numbered $1, \ldots, r$ and a program with l lines numbered $1, \ldots l$, where each line in the program has one of the following forms[1] :

   - `GOTO LINE j`
   - `IF REGISTER j > 0 GOTO LINE k`
   - `INCREMENT REGISTER j`

[1] Recall that incrementing a register means increasing its value by 1 and decrementing a register means decreasing its value by 1.

- `DECREMENT REGISTER j`
- `HALT`

We may assume that we never decrement a register containing 0, since we may always preface a decrement command by a command checking first that the value of the register is 0. Let R be the set of $x_1, \ldots, x_r$ such that the machine halts when register i is initialized to x_i. We show that R is diophantine.

The equation we will use to show that R is diophantine will begin by quantifying over parameters $Q,\ s,\ I,\ R_1, \ldots, R_r,\ y_1, \ldots, y_r,\ L_1, \ldots, L_l$, where we intend:

- $Q = 2^{x_1+\ldots+x_r+s+l+1}$ is a large power of 2 that we use as a base relative to which we can represent sequences of numbers.
- $I = \sum_{t=0}^{s} Q^t$ is the number having a 1 in every digit in base Q, and has length $s+1$.
- s is the number of steps the machine runs for.
- R_i is a number so that in base Q, the tth digit of R_i is the contents of the ith register at time t.
- y_i is the contents of the ith register at step s.
- L_i is a number so that in base Q, then tth digit of L_i is equal to 1 if the program is at line i at time t and is equal to 0 otherwise.

(a) (5 pts) Show that the definitions we have given for Q and I in terms of $x_1 \ldots, x_r, s, l$ are diophantine (assuming exponentiation is diophantine). [Hint: use the equation $1 + (Q-1)I = Q^{s+1}$ to define I]

(b) (5 pts) Show that the condition $R \preceq (Q/2-1)I$ forces that R must have at most $s+1$ digits in base Q, and that this relation is diophantine.

(c) (5 pts) Show that the conditions $L_1 \preceq I \wedge \ldots \wedge L_l \preceq I$, $1 \preceq L_1$ and $I = L_1 + \ldots + L_l$ force that for each t with $0 \leq t \leq s$, there is exactly one L_i such that the tth digit of L_i in base Q is 1, and the rest are 0, and the first digit of L_1 is 1.

(d) (5 pts) Show that $QL_i \preceq L_j$ corresponds to the ith line of the program being `GOTO LINE j`.

(e) (5 pts) Show that $QL_i \preceq L_k + L_{i+1}$ and $QL_i \preceq L_k + QI - 2R_j$ corresponds to the ith line of the program being `IF REGISTER j > 0 GOTO LINE k`.

(f) (5 pts) Let N be the set of pairs (i,j) such that line i in the program increments register j and let D be the set of pairs (i,j) such that line i in the program decrements register j. Show that for each i and j

$$R_j + y_j Q^{s+1} = QR_j + x_j + \sum_{(i,j)\in N} L_i - \sum_{(i,j)\in D} L_i$$

and the condition $QL_i \preceq L_{i+1}$ corresponds to the commands `INCREMENT REGISTER j` or `DECREMENT REGISTER j` being on line i.

(g) (10 pts) Finish proving the DPRM theorem.

3. (10 pts) (No collab) Show that if $A_0, A_1, A_2, \ldots \subseteq \mathbb{N}$ is a countable sequence of subset of $\mathbb{N}$, then there is some $B \subseteq \mathbb{N}$ such that for every i, $B \geq_T A_i$.

4. (20 pts) Show that if $A, B \subseteq \mathbb{N}$ and $A \leq_T B$, then $A' \leq_T B'$.