Homework 6

Chris Powell

A. Write a program that takes as input positive integers n and b, and returns n in base b. The output can be a list of digits. You may assume $b \leqslant 10$.

```
def baseb(n, b):
    """Given positive integers n and b, return n in base b"""
    d = []
    while n:  # while n not 0
        d += [n % b]
        n //= b
    return d[::-1]  # Return reversed list
```

Proof. Let n_i be the value of n after the i^{th} iteration, and let b be the fixed value of b. Then at each iteration, n_{i+1} is the quotient when n_i is divided by b. By the Quotient-Remainder Theorem, there exists unique integers q_i and r_i where $0 \leqslant r_i < b$. Hence $n_{i+1} = \frac{n_i - r_i}{b}$. Since $0 < b \leqslant n_i$, we know $0 \leqslant r_i < n_i$. Thus (n_i) is a strictly decreasing sequence of nonnegative integers. So there is some k for which $n_k = 0$. But this is this is the termination condition, so the program ends. We proved in class that for each n_i there exists a unique $t, d_0, d_1, \ldots, d_t$ such that $n_i = \sum_{i=0}^{t} d_i b^i$, where $0 \leqslant d_i < b - 1$ for all i. The correctness of the algorithm follows. $\square$

B. Silverman 9.1 Use Fermat's Little Theorem to perform the following tasks.

(a) Find a number $0 \leqslant a < 73$ with $a \equiv 9^{794} \pmod{73}$.

Obseve that

$$\begin{aligned}
9^{749} &\equiv 9^{10(73)+64} \pmod{73} \\
&\equiv \left(9^{73}\right)^{10} \cdot 9^{64} \pmod{73} \\
&\equiv 9^{10} \cdot 9^{64} \pmod{73} && \text{(Fermat's Little Theorem)} \\
&\equiv 9^{74} \pmod{73} \\
&\equiv 9^{1(73)+1} \pmod{73} \\
&\equiv 9^{73} \cdot 9 \pmod{73} \\
&\equiv 9 \cdot 9 \pmod{73} && \text{(Fermat's Little Theorem)} \\
&\equiv 81 \pmod{73} \\
&\equiv 8 \pmod{73}.
\end{aligned}$$

So take $a = 8$.

(b) Solve $x^{86} \equiv 6 \pmod{29}$

We have that

$$\begin{aligned}
x^{86} &\equiv x^{2(29)+28} \pmod{29} \\
&\equiv \left(x^{29}\right)^{2} \cdot x^{28} \pmod{29} \\
&\equiv x^{2} \cdot x^{28} \pmod{29} && \text{(Fermat's Little Theorem)} \\
&\equiv x^{30} \pmod{29} \\
&\equiv x^{1(29)+1} \pmod{29} \\
&\equiv x^{29} \cdot x \pmod{29} \\
&\equiv x \cdot x \pmod{29} && \text{(Fermat's Little Theorem)} \\
&\equiv x^{2} \pmod{29}.
\end{aligned}$$

But $6 \equiv 64 \pmod{29}$ and 64 is a perfect square, so $x^2 \equiv 64 \pmod{29}$. Therefore $x^{86} \equiv 6 \pmod{29}$ has incongruent solutions [8] and $[-8] = [21]$.

(c) Solve $x^{39} \equiv 3 \pmod{13}$.

Observe that

$$\begin{aligned} x^{39} &\equiv x^{3(13)+0} \pmod{13} \\ &\equiv \left(x^{13}\right)^3 \pmod{13} \\ &\equiv x^3 \pmod{13} && \text{(Fermat's Little Theorem)} \end{aligned}$$

But

$$\begin{aligned}
1^3 &\equiv 1 \not\equiv 3 \pmod{13} \\
2^3 &\equiv 8 \not\equiv 3 \pmod{13} \\
3^3 &\equiv 27 \equiv 1 \not\equiv 3 \pmod{13} \\
4^3 &\equiv 4^2 \cdot 4 \equiv 16 \cdot 4 \equiv 3 \cdot 4 \equiv 12 \not\equiv 3 \pmod{13} \\
5^3 &\equiv 5^2 \cdot 5 \equiv 25 \cdot 5 \equiv 12 \cdot 5 \equiv 60 \equiv 8 \not\equiv 3 \pmod{13} \\
6^3 &\equiv 6^2 \cdot 6 \equiv 36 \cdot 6 \equiv 10 \cdot 6 \equiv 60 \equiv 8 \not\equiv 3 \pmod{13} \\
7^3 &\equiv 7^2 \cdot 7 \equiv 49 \cdot 7 \equiv 10 \cdot 7 \equiv 70 \equiv 5 \not\equiv 3 \pmod{13} \\
8^3 &\equiv 8^2 \cdot 8 \equiv 64 \cdot 8 \equiv 12 \cdot 8 \equiv 96 \equiv 5 \not\equiv 3 \pmod{13} \\
9^3 &\equiv \left(3^3\right)^2 \equiv 1^2 \equiv 1 \not\equiv 3 \pmod{13} \\
10^3 &\equiv (2 \cdot 5)^3 \equiv 2^3 \cdot 5^3 \equiv 3 \cdot 8 \equiv 12 \not\equiv 3 \pmod{13} \\
11^3 &\equiv 11^2 \cdot 11 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \equiv 5 \not\equiv 3 \pmod{13} \\
12^3 &\equiv (3 \cdot 4)^3 \equiv 3^3 \cdot 4^3 \equiv 1 \cdot 12 \equiv 12 \not\equiv 3 \pmod{13}
\end{aligned}$$

Thus $x^{39} \equiv 3 \pmod{13}$ has no solution.

C. Silverman 9.2 The quantity $(p-1)! \pmod{p}$ appeared in our proof of Fermat's Little Theorem, although we didn't need to know its value.

(a) Compute $(p-1)! \pmod{p}$ for some small values of p, find a pattern, and make a conjecture.

p	$(p-1)!$	$(p-1)! \pmod n$
2	1	1
3	2	2
5	6	4
7	720	6

Conjecture. Let p a prime integer. Then

$$(p-1)! \equiv p-1 \pmod p.$$

(b) Prove that your conjecture is correct.

Lemma. Let p be a prime integer and let

$$S = \{ x \in \mathbb{Z} \mid 2 \leqslant x \leqslant p-1 \}.$$

Then for every $a \in S$, there is a unique $b \in S$, with $b \neq a$, such that $ab \equiv 1 \pmod p$.

Proof. Let $a \in \mathbb{Z}$. Then by the Linear Congruence Theorem, we know such a unique $b \in S$ exists. We show by contradiction that a and b are distinct. Suppose otherwise. Then $a^2 \equiv 1 \pmod p$ which implies $a^2 - 1 \equiv 0 \pmod p$. Thus

$$p \mid a^2 - 1 = (a+1)(a-1).$$

So either $p \mid a+1$ or $p \mid a-1$ since p is prime. But if $p \mid a+1$, then we have $a \equiv -1 \pmod p$, a contradiction. Otherwise, $a \equiv 1 \pmod p$, another contradiction. □

Proposition. Every prime integer satisfies

$$(p-1)! \equiv p-1 \pmod p.$$

Proof. It follows from the above that lemma that

$$(p-2)(p-3)\cdots(3)(2) \equiv 1 \pmod p.$$

Multiplying both sides of the congruence by $p-1$ proves the conjecture. □

D. Silverman 10.2 The number 3750 satisfies $\phi(3750) = 1000$. Find a number a that has the following properties:

(i) $a \equiv 7^{3003} \pmod{3750}$.

(ii) $1 \leqslant a \leqslant 5000$.

(iii) a is not divisible by 7.

Since

$$\begin{aligned}
\phi(3750) &= \phi(2)\phi(3)\phi\left(5^4\right) && \text{(Theorem 11.1 part (b))}\\
&= (2-1)(3-1)(5^4-5^3) && \text{(Theorem 11.1 part (a))}\\
&= 1 \cdot 2 \cdot 500\\
&= 1000,
\end{aligned}$$

we conclude that 3750 does indeed satisfy $\phi(3750) = 1000$. So, by Euler's formula, for any integer a, with $\gcd(a, 3750) = 1$,

$$a^{\phi(3750)} \equiv a^{1000} \equiv 1 \pmod{3750}.$$

In particular, $7^{1000} \equiv 1 \pmod{3750}$. But

$$\begin{aligned}
7^{3003} &\equiv 7^{3000} \cdot 7^3 \pmod{3750}\\
&\equiv \left(7^{1000}\right)^3 \cdot 7^3 \pmod{3750}\\
&\equiv 1 \cdot 7^3 \pmod{3750}\\
&\equiv 7^3 \pmod{3750}\\
&\equiv 343 \pmod{3750}.
\end{aligned}$$

Note that 343 satisfies (i) and (ii). Now since we also require $7 \nmid a$, take $a = 343 + 3750 = 4093$.

E. Let p be a prime, and suppose $\gcd(a, p) = 1$. Show that if $ax \equiv c \pmod{p}$, then $x \equiv ca^{p-2} \pmod{p}$.

Proof. Assume $ax \equiv c \pmod{p}$. Then $axa^{p-2} \equiv ca^{p-2}$. So $xa^{p-1} \equiv ca^{p-2} \pmod{p}$. But since $\gcd(a, p) = 1$, we know $a \not\equiv 0 \pmod{p}$. Therefore, Fermat's Little Theorem implies $xa^{p-1} \equiv x \cdot 1$. Hence $x \equiv ca^{p-2} \pmod{p}$. $\square$

F. Suppose $\gcd(x, 97) = 1$. Suppose $x^n \equiv 1 \pmod{97}$, where $1 \leqslant n \leqslant 96$, and furthermore suppose that n is the smallest number with these properties. Show that $n \mid 96$.

Proof. Since $\gcd(x, 97) = 1$, we know $x \not\equiv 0 \pmod{97}$. So Fermat's Little Theorem implies $x^{96} \equiv 1 \pmod{97}$. The Quotient-Remainder Theorem implies that $96 = qn + r$ for some unique $q, r \in \mathbb{Z}$, where $0 \leqslant r < n$. So

$$\begin{aligned} 1 &\equiv x^{qn+r} \\ &\equiv (x^q)^n \cdot x^r \\ &\equiv 1^n \cdot x^r && (\text{since } x^n \equiv 1 \pmod{97}) \\ &\equiv 1 \cdot x^r \\ &\equiv x^r. \end{aligned}$$

But this contradicts the minimality of n. □

G. Let $p(x) = x^{33} - x$. Show that if n is an integer, then $15 \mid p(n)$.

Note that $\gcd(n, 15) = g$ for $g \in \{1, 3, 5, 15\}$

H. Suppose a, n are integers with $n \neq 0$ and $\gcd(a, n) \neq 1$. Show that $a^r \not\equiv 1 \pmod{n}$ for any positive r.