1. Use mathematical induction to show that $3^n < n!$ for $n \geq 7$.

**Solution** We check that this inequality is satisfied for $n = 7$. Suppose that it is true for some $n \geq 7$. Then 
\[(n + 1)! = (n + 1) \cdot n! > (n + 1) \cdot 3^n > 3 \cdot 3^n = 3^{n+1}.
\]

2. Show that if $n$ is a positive integer then $(n + 1, n^2 - n + 1)$ is either 1 or 3.

**Solution** Suppose $d \mid n + 1$ and $d \mid n^2 - n + 1$. Then 
\[d \mid (n^2 - n + 1) - (n + 1)(n - 2) = 3
\]
and so $d = 1$ or $d = 3$. It is easy to check that either can occur.

3. How many solutions does the congruence $x^2 + 7x + 10 \equiv 0 \pmod{11}$ have? If there are any, find them all.

**Solution** Factoring 
\[(x + 2)(x + 5) \equiv 0 \pmod{11},
\]
and hence $x \equiv -2, -5 \pmod{11}$ (i.e. two solutions).

4. Use the Euclidean algorithm to express $(2128, 8316)$ as a linear combination of 2128 and 8316.

**Solution** We have 
\[8316 = 3 \cdot 2128 + 1932, \quad 2128 = 1 \cdot 1932 + 196, \]
\[1932 = 9 \cdot 196 + 168, \quad 196 = 1 \cdot 168 + 28, \]
\[168 = 6 \cdot 28.
\]
Putting this back together 
\[(2128, 8316) = 28 = 196 - 168 = 10 \cdot 196 - 1932 = 10 \cdot 2128 - 11 \cdot 1932
\]
and so 
\[(2128, 8316) = 43 \cdot 2128 - 11 \cdot 8316.
\]

5. Use Euler’s theorem to evaluate $2^{100000} \pmod{77}$.

**Solution** We have $\phi(77) = 60 = 2^2 \cdot 3 \cdot 5$ and 
\[100000 \equiv 0 \pmod{20} \text{ and } 100000 \equiv 1 \pmod{3}.
\]
We thus have that $100000 \equiv 40 \pmod{60}$ and so 
\[2^{100000} \equiv 2^{40} \pmod{77}.
\]
Since 
\[2^{40} \equiv (2^3)^{13} \cdot 2 \equiv 2 \pmod{7}
\]
and
\[ 2^{40} \equiv (2^5)^8 \equiv 1 \mod 11, \]
it follows that
\[ 2^{100000} \equiv 23 \mod 77. \]

6. Given \( N = p \cdot q = 3127 \), produce complete public and private keys for the RSA cryptosystem.

**Solution** To do this problem, we must first factor \( N = 53 \cdot 59 \), say by Fermat factorization. We thus have \( \phi(N) = 52 \cdot 58 = 2 \cdot 23 \cdot 13 \cdot 29 \).

We now choose some \( e > 1 \) coprime to this number, say \( e = 3 \), then solve \( 3d \equiv 1 \mod \phi(N) \), to find \( d = 2011 \). It follows that complete public and private keys are given by \((3, 3127)\) and \((2011, 3127)\), respectively.

7. Let \( N = a_m10^m + a_{m-1}10^{m-1} + \cdots + a_110 + a_0 \) be the decimal expansion of \( N \) (i.e. with \( 0 \leq a_i \leq 9 \) for each \( i \)) and let \( T = a_0 - a_1 + a_2 - \cdots + (-1)^{m}a_m \). Prove that \( 11 \mid N \) if and only if \( 11 \mid T \).

**Solution** We have
\[ N \equiv a_m(-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_1(-1)^1 + a_0 \equiv T \mod 11 \]
whereby the result is immediate.

8. Factor 8051 and 11413 using (a) Fermat factorization; (b) Pollard rho; and (c) Pollard \( p - 1 \).

**Solution** a) \( 90^2 - 8051 = 49 = 7^2 \), so we have \( 8051 = 83 \cdot 97 \). \( 107^2 - 11413 = 36 = 6^2 \), so \( 11413 = 101 \cdot 113 \).

b) Using \( f(x) = x^2 + 1 \) and a seed of \( x_0 = 2 \), we have, for \( N = 8051 \), that
\[ x_1 = 5, x_2 = 26, x_3 = 677, x_4 = 7474, x_5 = 2839, x_6 = 871 \]
and \((x_6, x_3, N) = 97\) which leads to the preceding factorization. Similarly, for \( N = 11413 \), we have
\[ x_1 = 5, x_2 = 26, x_3 = 677, x_4 = 1810, x_5 = 570, x_6 = 5337, x_7 = 8135, x_8 = 5652, \text{ and } (x_8 - x_4, N) = 113. \]

c) We find that
\[ (2^{64} - 1, 8051) = 97 \text{ and } (2^{77} - 1, 11413) = 113. \]

9. (Hard!) Show that if \( n \geq 2 \) is an integer, then \( n \) does not divide \( 2^n - 1 \).

**Solution** Suppose we have that \( 2^n \equiv 1 \mod n \) and let \( p \) be the smallest prime divisor of \( n \). Note that \( p > 2 \). Define \( d \) to be the smallest positive integer such that \( 2^d \equiv 1 \mod p \). Then we necessarily
have that $d \mid p - 1$. Since also $2^n \equiv 1 \pmod{p}$, we have that $d \mid n$ and so $d$ is a common divisor of $n$ and $p - 1$, contradicting the fact that every prime divisor (and hence nontrivial divisor) of $n$ is at least $p$.

10 Prove that 17 divides $11^{104} + 1$.

**Solution** Via Fermat’s Little Theorem,

$$11^{104} = (11^{16})^6 \cdot 11^8 \equiv 121^4 \equiv 2^4 \equiv 16 \pmod{17}$$

and so

$$11^{104} + 1 \equiv 0 \pmod{17}.$$ 

11 Let $p$ be a prime and $\gcd(a, p) = 1$. Prove that $x \equiv a^{p-2}b \pmod{p}$ is a solution of the linear congruence $ax \equiv b \pmod{p}$.

**Solution** This is an immediate consequence of Fermat’s Little Theorem.

12 Find an integer having the remainders 1, 2, 5, 5 when divided by 2, 3, 6, 12, respectively (Yih-hing, died 717).

**Solution** We wish to solve

$$x \equiv 1 \pmod{2}, \ x \equiv 2 \pmod{3}, \ x \equiv 5 \pmod{6}$$

and $x \equiv 5 \pmod{12}$. Notice that $x = 5$ works and since the least common multiple of 2, 3, 6 and 12 is 12, the general solution is just $x \equiv 5 \pmod{12}$.

13 Mimic Euclid’s proof to show that there are infinitely many primes of the shape $8k + 7$.

**Solution** Apologies for this one – Euclid’s proof really doesn’t work here! The actual proof is rather more involved – I will omit it.

14 Show that the only solutions of the equation $3^x - 2^y = 1$ in positive integers $x$ and $y$ are with $(x, y) = (1, 1)$ or $(x, y) = (2, 3)$.

**Solution** Notice the typo – the second solution should be $x = 2, y = 3$. In any case, we check that the only solutions with $y \leq 3$ are the two known ones. If $y \geq 3$ then it follows that $3^x \equiv 1 \pmod{8}$ and so $x$ is even, say $x = 2x_0$ for $x_0$ a positive integer. Then

$$3^x - 1 = 3^{2x_0} - 1 = (3^{x_0} - 1)(3^{x_0} + 1) = 2^y.$$ 

Since $\gcd(3^{x_0} - 1, 3^{x_0} + 1) = 2$, it follows that $3^{x_0} - 1 = 2$ and $3^{x_0} + 1 = 4$, so that $x = 2$.

15 Find the largest positive integer $k$ such that $k!$ can be written as the sum of two integer squares.
Solution The largest such $k$ is $k = 6$, where $6! = 24^2 + 12^2$. For larger $k$ it is possible to show (not so easy – this is actually a variant of something rather hard called Bertrand’s Postulate!) that there exists a prime $p \equiv 3 \mod 4$ with $k/2 < p \leq k$. Such a prime necessarily divides $k!$ to the first power.