IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises V.

1. *Extended Euclidean algorithm* is arguably the most important algorithm in number theory.
   (a) Use the Euclidean algorithm to find the gcd$(3033, 1685)$.
   (b) Use the extended Euclidean algorithm to find an inverse of 333 in $(\mathbb{Z}_{499}, \cdot)$.
2. Bob sets up the Knapsack cryptosystem with $X = (2, 7, 10, 20, 42, 90)$, $m = 313$, $u = 27$ so that Alice can send him messages.
   (a) Find Bob's public key X'.
   (b) Encode the message 101101 and 010010.
   (c) Perform in detail Bob's decryption of $c_1 = 310$ and $c_2 = 238$.
3. Consider the RSA cryptosystem with public modulus $n = 1189$ and encryption exponent $e = 9$. You have obtained the following *(plaintext, cryptotext)* pairs:

   $$(19, 1113), \quad (29, 522), \quad (39, 308).$$

   Use this knowledge to decrypt the cryptotext $c = 377$ without factoring n.
4. Factor 289651 using the fact that $\phi(289651) = 287712$ and knowing that it has two factors.
5. Show that any super-increasing vector $(x_1, x_2, \ldots, x_n)$ must satisfy $x_i \geq 2^{i-1}$ for all $i = 1, 2, \ldots, n$.
6. Prove that for any prime $p > 5$ it holds that $120 \mid p^4 - 1$.
7. Bob and Alice used the same public modulus $n = 2867$ to set up RSA with their respective public keys being $e_A = 2677$ and $e_B = 499$. You managed to obtain Alice's private key $d_A = 133$. Without factoring n, decrypt the cryptotext $c = 2094$ which was sent to Bob.