Problem Set 3 — Number theory

1. Find the last two digits of

$$2^{2026}.$$

2. Find the last digit of

$$7^{7^{7^7}}.$$

3. Find the fifth digit from the right of

$$5^{5^{5^{5^5}}}$$

4. Let the sequence $(a_n)_{n\in\mathbb{N}}$ be defined by

$$a_1 = 7, \qquad a_{n+1} = 7^{a_n}, \quad n \in \mathbb{N}.$$

Let

$$b_n = a_n \bmod 100, \qquad n \in \mathbb{N}.$$

Find all integers that occurs in the sequence $(b_n)_{n\in\mathbb{N}}$ infinitely many times.

5. The same message m was encrypted using the RSA cryptosystem for three recipients with public keys

$$(n_i, e), \qquad i = 1, 2, 3,$$

where

$$n_1 = 856205355226618825334201920757106189619224699081629760978379,$$
$$n_2 = 132898970305754951343691562182508528785465374943270095921804 7,$$
$$n_3 = 454354335307926896909207147444504297415186755348139088337797$$

and $e = 3$ (all recipients use the same exponent e). The corresponding ciphertexts are

$$\hat{m}_1 = 740425793465388555119503964648476369739800418029540350718050,$$
$$\hat{m}_2 = 379024675447467155328545229780563222680646766208695846228599,$$
$$\hat{m}_3 = 411198195497414070662759224293482345584589805255958400512866.$$

Decipher the message m. Is it possible to recover m using only two triples $(n_i, e, \hat{m}_i)$? Why or why not?

6. The RSA public key is

$$n = 131351596182359481557515491331585220774738647194168655490775097 8089,$$
$$e = 339524092801641188288639324893649122277738024720460821469318659 87.$$

Knowing that the corresponding private exponent is

$$d = 916068662416111846290622300265918825790030273088625292735182448923$$

find the prime factorization of n.

7. Bob's RSA key generation was flawed because he chose two primes p and q whose difference is too small. His public key in the RSA cryptosystem is

$$n = 210656975655260502837093406173594832261292526082633758681180386 21,$$
$$e = 162937774898941868463580325891965275001955210686672781079373104 71.$$

Find Bob's private key.