

## Homework 4 Solutions

2.6 # 31: The example in the book passes because all the powers computed are  $\equiv 1$ . For the version I suggested,  $25 = 5^2$  is of course also composite. Write  $24 = 25 - 1$  as  $2^3 \cdot 3$  and compute  $7^3 \equiv 18 \pmod{25}$ ,  $7^6 \equiv 24 \equiv -1$ ,  $7^{12} \equiv 1$ ,  $7^{24} \equiv 1$ . This passes because the last power that is not  $\equiv 1$  is  $\equiv -1$ .

2.6 # 32: Factor  $1729 = 7 \cdot 13 \cdot 19$ . If  $x$  is relatively prime to 1729, then  $x^{1728} = (x^6)^{288} \equiv 1 \pmod{7}$ , by Fermat's theorem. Similarly,  $x^{1728} = (x^{12})^{144} \equiv 1 \pmod{13}$  and  $x^{1728} = (x^{18})^{96} \equiv 1 \pmod{19}$ . By the Chinese remainder theorem, it follows that  $x^{1728} \equiv 1 \pmod{1729}$ .

The number 1729 figures in an oft-repeated story about the mathematicians Hardy and Ramanujan. Hardy visited Ramanujan in the hospital and remarked that his taxicab was number 1729, which didn't seem like a particularly interesting number. Ramanujan, however, pointed out immediately that  $1729 = 10^3 + 9^3 = 12^3 + 1^3$  is the smallest number that is a sum of two cubes in two different ways. He probably didn't know that it is also a Carmichael number.

2.6 #46, 47: ATTACK encrypts as 2299 1317 2117. The exponent  $d$  for decrypting is 937.