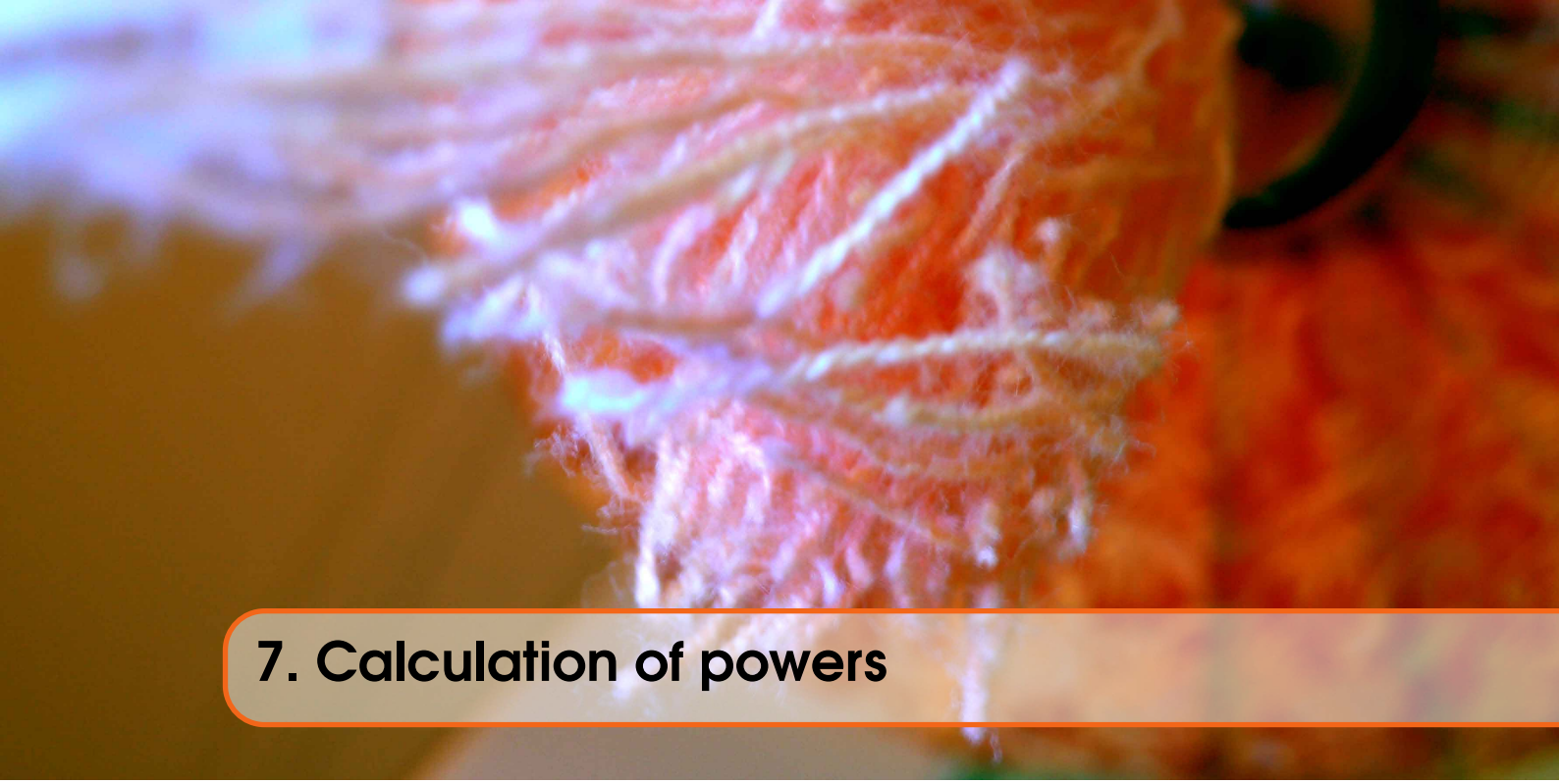

7. Calculation of powers

To calculate 4^{30} on a 7-hour clock it would be inelegant, and inefficient, to do the following.

$$\begin{aligned} 4^{30} &= 1152921504606846976 && (7.1)\\ &= 1 + 7 \times 164703072086692425 && (7.2)\\ &\equiv 1 \mod 7 && (7.3) \end{aligned}$$

There is a more elegant approach.

$$\begin{aligned} 4^{30} &= ((4^2)^3)^5 && (7.4)\\ &\equiv (2^3)^5 \mod 7 && (7.5)\\ &\equiv 1^5 \mod 7 && (7.6)\\ &\equiv 1 \mod 7 && (7.7) \end{aligned}$$

To calculate 38^{75} on a 103-hour clock we could procede as follows.

$$\begin{aligned} 38^{75} &= 38^{(64+8+2+1)} && (7.8)\\ &= 38(38^2)(38^8)(38^{64}) && (7.9)\\ &\equiv 38(2)(2^4)(2^{32}) \mod 103 && (7.10)\\ &\equiv 76(2^4)(2^8)^4 \mod 103 && (7.11)\\ &\equiv 76(2^4)(50)^4 \mod 103 && (7.12)\\ &\equiv 76(-3)^4 \mod 103 && (7.13)\\ &\equiv 76 \times 81 \mod 103 && (7.14)\\ &\equiv 79 \mod 103 && (7.15) \end{aligned}$$

These are useful tricks for calculating powers in clock arithmetic, though not too exciting from a mathematical viewpoint.

7.1 Euler's theorem

The following result is useful and, on first encounter, probably quite surprising.

Theorem 7.1.1 — Euler's theorem. If m and a are coprime positive integers, then

$$a^{\phi(m)} \equiv 1 \mod m .$$

To illustate the theorem for $a = 4$, $m = 9$ we calculate $\phi(9) = 6$ and note:

$$\begin{aligned} 4^6 &\equiv (4^2)^3 \mod 9 && (7.16)\\ &\equiv 7^3 \mod 9 && (7.17)\\ &\equiv 1 \mod 9 && (7.18) \end{aligned}$$

Euler's theorem is useful for calculating powers in clock arithmetic. To illustrate this let us calculate $2^{1\,000\,000} \mod 77$. First we calculate $\phi(77)$.

$$\begin{aligned} \phi(77) &= \phi(7 \times 11) && (7.19)\\ &= \phi(7)\phi(11) && (7.20)\\ &= 6 \times 10 && (7.21)\\ &= 60 && (7.22) \end{aligned}$$

Next we calculate the power.

$$\begin{aligned} 2^{1\,000\,000} &= (2^{60})^{16666} 2^{40} && (7.23)\\ &\equiv 1^{16666} 2^{40} \mod 77 && (7.24)\\ &\equiv (2^8)^5 \mod 77 && (7.25)\\ &\equiv 25^5 \mod 77 && (7.26)\\ &\equiv 9 \times 9 \times 25 \mod 77 && (7.27)\\ &\equiv 23 \mod 77 && (7.28) \end{aligned}$$

We shall prove a special case of Euler's theorem and then leave the reader to try to extend this proof to the general case.

7.2 Fermat's little theorem

By taking $m = p$ a prime in Euler's theorem, and noting that $\phi(p) = p - 1$, we arrive at the following result of Pierre de Fermat.

Theorem 7.2.1 — Fermat's little theorem. For a prime p and integer a not divisible by p the equation

$$a^{p-1} \equiv 1 \mod p$$

holds.

To explain why Fermat's little theorem is true, let a and p be integers satisfying the hypothesis of the theorem. Consider the numbers

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a \mod p \qquad (7.29)$$

on a p-hour clock. We claim that no two numbers in this list are equal. For if two of the numbers in the list, say $i.a$ and $j.a$, were the same modulo p then:

$$i.a - j.a \equiv 0 \mod p \qquad (7.30)$$

This would imply:

$$(i-j)a \equiv 0 \mod p \tag{7.31}$$

Thus $(i-j)a$ would be divisible by p. Since a is coprime to p this would mean that p divides (i-j). That in turn would mean

$$(i-j) \equiv 0 \mod p \tag{7.32}$$

and consequently:

$$i \equiv j \mod p \tag{7.33}$$

But since $1 \leq i, j < p$, we would then have $i = j$. Thus numbers in the list (7.29) are distinct from each other.

On taking the product of the numbers in the list, we find:

$$(a)(2a)(3a)\cdots((p-1)a) = 1 \times 2 \times 3 \times \cdots \times (p-1)a^{p-1} \tag{7.34}$$

$$\equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \mod p \tag{7.35}$$

This implies

$$a^{p-1} \equiv 1 \mod p \tag{7.36}$$

as required.

7.3 In readiness for RSA cryptography

The following application of Euler's theorem will be needed for a discussion of RSA cryptography.

Lemma 7.3.1 Let p and q be distinct prime numbers. Let e be an integer which is not divisible be either p or q, and set

$$d = e^{-1} \mod (p-1)(q-1)\ ,$$

Then for any integer a that is not divisible by either p or q the equation

$$(a^e)^d \equiv a \mod pq$$

holds.

The lemma is proved by noting:

$$(a^e)^d = a^{ed} \tag{7.37}$$

$$= a^{1+k(p-1)(q-1)} \quad \text{for some integer } k \tag{7.38}$$

$$= a(a^{\phi(pq)})^k \tag{7.39}$$

$$\equiv a(1)^k \mod pq \quad \text{(by Euler's theorem)} \tag{7.40}$$

$$\equiv a \mod pq \tag{7.41}$$