1) a) Euclid's gcd algorithm guarantees the *existence* of prime factorisations, on which RSA is based (via FTA);

b) Bézout's lemma may be used to compute the multiplicative inverse d of e or vice versa (step 2 of RSA on slide 10 of week 9), see slide 13 and below;

c) Fast exponentiation (in its modular form) may be used both for encrypting (step 3) and decrypting (step 4) messages;

d) The Chinese remainder theorem may be used to speed up encoding (step 3) and decoding (step 4) by exponentiation, by working modulo factors instead of their product;

e) Fermat's little theorem guarantees decoding followed by encoding of a message m by means of exponentiation (step 3 followed by step 4), yield the identity, i.e. yields m.

2) • We perform operations on prime factorisations, via the corresponding operations on the exponents of prime factors (slide 9 of lecture 9): $\gcd(\frac{2^3\cdot 3^1\cdot 2^5\cdot 5^4}{5^3}, 2\cdot 3^7\cdot 5^2) = \gcd(\frac{2^{3+5}\cdot 3^1\cdot 5^4}{5^3}, 2^1\cdot 3^7\cdot 5^2) = \gcd(2^8\cdot 3^1\cdot 5^{4-3}, 2^1\cdot 3^7\cdot 5^2) = 2^{\min(8,1)}\cdot 3^{\min(1,7)}\cdot 5^{\min(1,2)} = 2^1\cdot 3^1\cdot 5^1 = 30$;

• Since $60 = 2^2\cdot 3\cdot 5$ and $14 = 2\cdot 7$, we note $\gcd(60,14) = 2$, so that integers u and v such that $2 = u\cdot 60 + v\cdot 14$ can be found by Bézout's lemma (slide 4 of lecture 9):

$$\begin{aligned}
60 &= 1\cdot 60 + 0\cdot 14\\
14 &= 0\cdot 60 + 1\cdot 14\\
46 &= 1\cdot 60 - 1\cdot 14\\
32 &= 1\cdot 60 - 2\cdot 14\\
18 &= 1\cdot 60 - 3\cdot 14\\
4 &= 1\cdot 60 - 4\cdot 14\\
10 &= -1\cdot 60 + 5\cdot 14\\
6 &= -2\cdot 60 + 9\cdot 14\\
2 &= -3\cdot 60 + 13\cdot 14
\end{aligned}$$

That is, we may take $u = -3$ and $v = 13$. We verify: $-3\cdot 60 + 13\cdot 14 = -180 + 182 = 2$.

• Since $\gcd(9,11) = 1$ as one easily checks, 9 does have some inverse x modulo 11 and it can be computed using Bézout's lemma (slide 13 of lecture 9). From that we obtain $1 = 5\cdot 9 - 4\cdot 11$, so that 5 is the answer. We verify $9\cdot 5 \equiv 45 \equiv 1 \pmod{11}$.[1]

• By the Chinese remainder theorem (RSA version, slide 20 of lecture 9), a natural number $0 \le x < 9\cdot 11$ such that $x \equiv 4 \pmod 9$ and $x \equiv 5 \pmod{11}$ can be computed as $4 + 9\cdot((5\cdot(5-4)) \pmod{11}) = 49$, using that 5 is the inverse of 9 modulo 11, and that $\gcd(9,11)$, as established in the previous item.

3) • Since $m - 1 \equiv -1 \pmod m$ for any $m > 1$, and since then $-1\cdot -1 \equiv 1 \pmod m$, we have that $m - 1$ is its own inverse modulo m. (Note this does not depend on m being a prime number; e.g. $3\cdot 3 \equiv 1 \pmod 4$.) Therefore, 2016 is its own inverse modulo 2017.

[1] Alternatively: noting that 11 is a prime number, we have by FLT (slide 13 of lecture 9) that $9^{10} \equiv 1 \pmod{11}$, so that $9\cdot 9^9 \equiv 1 \pmod{11}$, i.e. 9^9 is the inverse of 9 modulo 11.

- 2015^{2016} is a 6662-digit number.[2]
- Since 2017 is a prime number and obviously $2017 \nmid 2015$, we have $2015^{2016} \equiv 2015^{2017-1} \equiv 1 \pmod{2017}$ by Fermat's little theorem.
- Since 2017 is prime and $2017 \nmid 2014$ we know by Fermat's little theorem that $2014^{(2015^{2016})} \equiv 2014^{(2015^{2016}) \bmod (2017-1)} \equiv 2014 \pmod{2017}$ using that $2015^{2016} \equiv (-1)^{2016} \equiv 1 \pmod{2016}$ as 2015 is its own inverse $(-1 \cdot -1 = 1)$ and 2016 is even.

4∗) If $\sim_1$ and $\sim_2$ are equivalence relations on a set A, then $(\sim_1)^{-1}$ is an equivalence relation as $\sim_1^{-1}$=$\sim_1$ by $\sim_1$ being symmetric, and $\sim_1^*$=$\sim_1$ as taking the reflexive–transitive closure of $*$ does not change it. Transitivity may fail for the union as exemplified by $\sim_1$= $\{(0,0),(0,1),(1,0),(1,1)\}$ and $\sim_2$= $\{(1,1),(1,2),(2,1),(2,2)\}$. Then 0 $(\sim_1 \cup \sim_2)$ 1 $(\sim_1 \cup \sim_2)$ 2 but 0 and 2 are not related by $\sim_1 \cup \sim_2$ Finally, $\sim_1 \cap \sim_2$ is an equivalence relation. To see the intersection preserves equivalence relations, note that we already know it preserves partial orderedness. Hence it suffices to show it preserves symmetry: $a\ (R \cap S)\ b$ iff $a\ R\ b$ and $a\ S\ b$ iff $b\ R\ a$ and $b\ S\ a$ iff $b\ (R \cap S)\ a$, for R,S symmetric relations.

[2] 2015^{2016} in decimal notation is

26212096726068930033035807074416328887868892226336241741496738334406468549876713728057176244882578312127216126927562769835305
36310750282770582211987195310573489887077601709261405344973251229295420381720923717595328332123953443920234825651842304892871
37783593594261834774278185721141763436300866406096047289192966018489401851676396399844092238698349769156568861423272966610082
11582326738883179540431811263858962149753242532488341906468774791474549558300495664138534579900234296427154644464094193950329
10018834061539929233969978020980385365155429061786577132877161389408995308012304811853925227439554650660305746886077173740988
86286228855791578744104825946220305089805428659354669334126090582974527704922400518599487432279860865417612273159455711970937
54698606707260714084620245985236711232249502705069965027734584305852352144640727302464245317282782610831150081015436267978915
91142442176802163376486663526196312686693291811487321045715150081525204885502197020668896540346418088054596642349279618554204
11661153145455405404112454714452058132410347091338844939949414400237355255787156933002827383186556770142613109167746962278402
51949761554729740991766062957923653373454949089928422897707992139865073665325246353151236059593575466160509787179578403321767
38164808783510912511716568076108063539966026953798882986865730508912238939021414747812005880780984690055011077375421395752047
03969759415011025689149015981840522589014043389353686174224740896760905169710248367754792535384391934707083242356251154027699
68907989775407495867591994607237862505633192789547196004935076908846380526412067204625299645919638245535423103137433020867484
62515632309664543599545259837681875958110952673188868946652372046232393694300832715218869265499592515028745889911567800791714
33886794731182701738908503870411620769318905856751484543070303035366082590354076658516877819106618063061756344071811186898030
97041047076357859340598292809931626987822277104707296202840477679022728175079244073589262908131172550276036044835073480509201
32617141674785353014562808350952521269392780310752606584217265082513281343985636549335899056428147655284095501686944492303936
46964722320238544702642295589111705812559044549860832491207459933484502318541536722579090651681944012139267432658558276413244
43057061909428688349660649895568321751855708875580160693373639945103133521145350275589939081765711825075019109985040573759316
36848982638386802868891682620660325859179506254244234892958863886005252737219191498719256083838048928782578121298797351064789
38087338080953999601753315035027958279878467617097074866226646635822907662736885601504344762193195485588684811869818713472647
85277834917558413879836303446922621161197722205665135595297196040644061520311721561299663657542238107250630020103612763879049
09307285392218960791468042720792300922908066040146364110293035747125458110296913825230985178179299069648576761496581825456576
90640001592179508060787759407085833487774091050387312275157079246909771221518646590238638408207501329881789915360301483806188
03944711714984992092676961870920266706320175896866691992158133806250717363710149915267205052627308141077824939873482503718874
53697933953689544707826344960956156080733821345221251774414173022077062212910265493214368172528086262210348134239640382248667
84665291810799761098412005155736215074284938453758651279873931071545504723024174382838266925055185265376438145799391254770542
32840620539756645086239053149517876744939534228658578687842794681690059373273532935287163470553296707723981239472683045399 74
18814143219973179231329408560025425967998899518452356686650950849375508299742179648178461643732494062165771980186899934896694
82898961475020516690642533934204983275665240793777309012789817760404347376154825107395122424966177430922714167039984851302726
91956401281650663605134228984324983079481619344849435930016584660595619150876547523785919737523392842178511390101882680184289
25785476910369784692555598681426172523191643025395942192253174316692175784352631416601448980071721089695699412423924160218588
79508862679544771488036827503520409920796127494205731927875436488530959712042656105816172452925011230188176635406242856065482
25210076753681162944573783539380927656838985558650530600975779189743141567945443765480587753179595178127117285834800701670134
87915846545813623320590331403792469806836246106259905284057604755269949626232604152667362093325732681178138928719404997422201
99051066829375909023932687229338181645632726586063552098997382222065291971974547123077054409493468415574833415277682208850374
21587407234972780435437772205884094180775079443006996214852370169835506264318869461951952406683412725778357078425248021466549
63997519982468449048517499602684461727426942461875291119735683400260150248981991924036897480835301134321799163115094242649789
72837768127746280663339985207856067286657210355661436893735816455630790380651645131219142962904413680910060352782411689044441
75992193638610032254036656913716979976007504460368986537094159773454801623861993005188452145931153635651317140013803007144 0
87716515273116696332482469296448886247387019573912947236754635176646543183645732017618817278760021264459905024379431832993795
15745296816460304105741544734005045908512668455594158953257761771604285469270132388270757844465986954365677349260470335344382
64478901872888514376980990010038688783271525731762444233135874607611724372614913132206022615881215704812452631107664169401015
83089834871092218655338310272237576913021055370381983755871927000720790933543793906847034756554844957043531379010837942735903
37598895223898652072788865169310908204861307409880189363730654639596641802059029698495883256290787977031156290258667526695977
21631849588256983229053467618350013851534302804328335769301726464976441528645487656088296656136094272605504872099462919568712
86713539991120920345558950706828311398049104483406194044766753459938075285269424373199959185491179532107944522315752813490436
00027169195364045830314785589202694218460862209086778191065174694644999028969244115963240768254869458771683609548128568438302
64508250091885699084878062975389367826438900668084046364751289137940079398152301698178204383017063332953778103125491942869 0
56036766537343856072352531821736229290095390524938357915012377506965228344676127433130608852944759551458820082533248820783745
61630416356077088428738603137628854859669713567256200910245249356932472850231311812463652837707045875600296038116647780054677
67464860622960636652166173277068760147704942279770305013061680308486557987686685241311389105629247316438068941909804610988287
99001496580700114372773625585173105012831178188429132323923004377362092260548638861234758638639636383081077110990667110388546
71222964043408865109086036682128906 25.