Lektionsförslag:

Centralt innehåll matematik 1b och matematik 1c:

Taluppfattning, aritmetik och algebra

- Egenskaper hos mängden av heltal, olika talbaser samt begreppen **primtal** och delbarhet.
- Metoder för beräkningar inom vardagslivet och karaktärsämnena med reella tal skrivna på olika former inklusive **potenser med heltalsexponenter** samt **strategier för användning av digitala verktyg**.

Centralt innehåll matematik 5:

Diskret matematik

- **Begreppet kongruens hos hela tal och kongruensräkning**.

Mål: Primtalstest och presentation av RSA
Förkunskaper: Potensräkneregler och modulräkning inkl räkneregler.
Tidsåtgång: 80 min eller 2·60 min

Inledning**:** Vi är omgivna av stora primtal. Chipet på kontokortet fungerar pga primtalens egenskaper. När vi betalar via Internet garanteras vår säkerhet med stora primtal. När jag skriver en digital signatur (t.ex. på deklarationen) är det stora primtal som ser till att det kan garanteras att det är jag som skriver på (om jag har behandlat koderna på ett säkert sätt).
Primtalen har studerats i århundraden men först i nyare tid har de fått flera praktiska användningsområden.

Aktivitet: Faktorisering av stora tal: t.ex. 2001 2002 2003 2005….
Svar:
2001=3*23*29
2002=2*7*11*13
2003 primtal (Sophie Germain primtal eftersom 2*2003+1= 4007 också är ett primtal)
2005 = 5*401

Diskussion: Hur gör jag och vilka tal kan ingå i faktoriseringen?

Fråga: Hur vet jag om ett tal är ett primtal? Jag behöver ett primtalstest.

Speciella potenser (beräkna och hitta mönster (viktigt att $sgd(a,p)=1$ om man tar flera exempel))
Dela gärna ut modulo-grupperna till eleverna i grupper *). Här är det viktigt att eleverna redan kan modulräkning.

$2^4 \ mod \ 5 =$	$2^6 \ mod \ 7 =$	$2^8 \ mod \ 9 =$
$3^4 \ mod \ 5 =$	$3^6 \ mod \ 7 =$	$3^8 \ mod \ 9 =$
$4^4 \ mod \ 5 =$	$4^6 \ mod \ 7 =$	$4^8 \ mod \ 9 =$
$2^{10} \ mod \ 11 =$	$2^{12} \ mod \ 13 =$	$2^{14} \ mod \ 15 =$
$3^{10} \ mod \ 11 =$	$3^{12} \ mod \ 13 =$	$3^{14} \ mod \ 15 =$
$4^{10} \ mod \ 11 =$	$4^{12} \ mod \ 13 =$	$4^{14} \ mod \ 15 =$

Svar

$2^4 \; mod \; 5 = 1$	$2^6 \; mod \; 7 = 1$	$2^8 \; mod \; 9 = 4$
$3^4 \; mod \; 5 = 1$	$3^6 \; mod \; 7 = 1$	$3^8 \; mod \; 9 = 0$
$4^4 \; mod \; 5 = 1$	$4^6 \; mod \; 7 = 1$	$4^8 \; mod \; 9 = 7$

$2^{10} \; mod \; 11 = 1$	$2^{12} \; mod \; 13 = 1$	$2^{14} \; mod \; 15 = 4$
$3^{10} \; mod \; 11 = 1$	$3^{12} \; mod \; 13 = 1$	$3^{14} \; mod \; 15 = 9$
$4^{10} \; mod \; 11 = 1$	$4^{12} \; mod \; 13 = 1$	$4^{14} \; mod \; 15 = 1$

I övningen ovan kan man utnyttja att t.ex.
$4^{14} = (2 \cdot 2)^{14} = 2^{14} \cdot 2^{14} \equiv \{redan \; beräknat\} \equiv 4 \cdot 4 = 16 \; \equiv 1 \; mod \; 15$

Fermats lilla sats: Om p är ett primtal och $sgd(a, p) = 1$ är $a^{p-1} \; mod \; p = 1$
(Pierre de Fermat 1601-1665 fransk amatörmatematiker; också känt för Fermats stora sats)

Speciellt: om $a^{p-1} \; mod \; p \neq 1$ för något a där $sgd(a, p) = 1$ är p INTE ett primtal.
Att vi fick $4^{14} \; mod \; 15 = 1$ betyder bara att 15 KANSKE är ett primtal.

****) Förslag till gruppindelning***: eleverna får ett heltal (= tal) mellan 1 och antal elever i klassen. Eleverna beräknar *(tal+100)tal mod 17*. Elever med samma moduls bildar grupp. Med 32 elever blir det 9 grupper om 2 till 4 elever.

Slutsats: Det är svårt att faktorisera sammansatta tal men det är ofta enkelt att avgöra om ett tal är ett primtal.

När man gör banktransaktioner via Internet vill man inte att känslig information kan läsas av andra än banken. Informationen måste alltså krypteras så bara den tilltänkta mottagaren kan läsa informationen. Det kan t.ex. göras med RSA-kryptering som offentliggjordes 1978 som utnyttjar att det är svårt att faktorisera stora tal. RSA är en såkallat ”öppen nyckel” kryptering där man offentliggör sina krypteringsnycklar.
RSA står för begynnelsebokstäverna i Rivers, Shamir och Adelman upphovsmännen till RSA. Se mera i RSA-kryptering av Torbjörn Tambour, SU.

RSA ett exempel:
Banken har offentliggjort sina nycklar som $n=143 \; e=7$ där n är produkten av två primtal p och q som Banken håller hemliga.
e är ett heltal som är relativ prima med $(p-1)(q-1)$ och $1 < e < (p-1)(q-1)$
Till nyckelparet finns en hemlig nyckel d. Spioner som kan bestämma Bankens hemliga nyckel d utifrån det offentliga nyckelparet kan läsa Bankens inkommande post.
Banken hemliga nyckel d uppfyller att $d \cdot e \equiv 1 \; mod \; (p-1)(q-1)$. Banken kan enkelt bestämma d eftersom Banken känner p och q och alltså också $(p-1)(q-1)$. Men eftersom faktorisering av n är svårt om n är stort (over 200 siffror) är det i praktiken bara Banken som kan bestämma d.

Om Alice vill skicka ett meddelande ”42” till Banken (detta kan vara en del av hennes kontonummer) krypterar hon mha Bankens offentliga nycklar: $42^7 \ mod \ 143 = 81$ och skickar ”81” till Banken.
När Banken mottar ”81” från Alice tar Banken sin hemliga nyckel $d=103$ och beräknar $81^{103} \ mod \ 143 = 42$ och kan läsa Alices kontonummer.

□

Aktivitet
Faktorisera 143 för att bestämma p och q så $143 = p \cdot q$.
Svar: $143 = 11 \cdot 13$.

Aktivitet
Undersök om $e=7$ är relativ prima med (p-1)(q-1) och att 1 < e < (p-1)(q-1).
Svar: e är ett primtal så $(p-1)(q-1)$ får inte vara delbart med 7: $(p-1)(q-1)=10 \cdot 12=120=2^3 \cdot 3 \cdot 5$ alltså är d relativ prima med $e=7$.

Aktivitet
Undersök om $d=103$ uppfyller att $d \cdot e \equiv 1 \ mod \ (p-1)(q-1)$.
Svar: $d \cdot e \equiv \ 7 \cdot 103 = 721 \equiv 1 \ mod \ 120$.

Om tiden tillåter kan man som en kuriositet nämna:
Fermatprimtal: Fermat sägs ha påstått att alla $F_i = 2^{2^i} + 1, \ \geq 0$ är primtal.

Aktivitet: Beräkna de första sex F_i och avgör om de är primtal.
$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$
$F_5 = 4294967297$

Svar:
$F_0 – F_4$ är alla primtal.
$3^{4294967296}$ ger rest 3029026160 vid division med F_5 = 4294967297 och vi kan med säkerhet säga att F_5 inte är ett primtal. Här är wolframalpha.com ett bra hjälpmedel. Fermat hade alltså fel (inga andra kända tal i serien är primtal). Även om WolframAlpha inte fanns på Fermats tid tar ovanstående algoritm endast någon timme att genomföra för hand om man är van.

***Extra aktivitet*:** Avgör om 143 är primtal.
Svar: Beräkna t.ex. $2^{142} \ mod \ 143 = 114$ och dra slutsatsen att 143 INTE är ett primtal.
$2^{142} = 2^{2 \cdot 71}$
$= 4^{71}$ ..... potenslag
$= 4^{1+2 \cdot 35}$ ..... division med 2 med rest
$= 4 \cdot (4^2)^{35}$ ..... potenslag
$= 4 \cdot (16)^{1+2 \cdot 17}$ ..... division med 2 med rest
$= 4 \cdot 16 \cdot (16^2)^{17}$
$= 64 \cdot 256^{1+2 \cdot 8}$
$= 64 \cdot 256 \cdot (256^2)^8$
$= 16384 * (65536)^8$

$\equiv_{143} 82 \cdot 42^8$ .....resträkning

$= 82 \cdot (42^2)^4$

$= 82 \cdot (1764)^4$

$\equiv_{143} 82 \cdot 48^4$ .....resträkning

$= 82 \cdot (48^2)^2$

$= 82 \cdot (2304)^2$

$\equiv_{143} 82 \cdot (16)^2$.....resträkning

$\equiv_{143} 114$ .....resträkning

Källor

Modulär aritmetik av Torsten Ekedahl, SU

Primtal, faktorisering och RSA av Johan Håstad, KTH

RSA-kryptering av Torbjörn Tambour, SU

Pierre de Fermat, Wikipedia

WolframAlpha